Lucent Technologies
Bell Labs Innovations

Navis ™ Optical Element Management System (EMS)

Administration Guide

Release 8.0

190-224-158R8.0
Issue 1.0
April 2002

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. Information is subject to change; however, Lucent Technologies assumes no responsibility for any errors that may appear in this document.

Mandatory customer information

FCC Warning Statement

This equipment generates, uses, and can radiate radio frequency energy. If not installed, used, and maintained in accordance with the instruction manual, it may cause interference to radio communications. Operation of this equipment in a residential area may cause interference, in which case users will be required to take whatever measures may be required to correct the interference at their own expense.

Trademarks

WaveStar is a registered trademark of Lucent Technologies.

INFORMIX is a registered trademark of Informix Software, Inc.

Lantronix is a registered trademark of Lantronix.

Microsoft is a registered trademark of Microsoft Corporation.

Windows is a trademark of Microsoft Corporation.

Hewlett-Packard is a registered trademark of Hewlett-Packard

HP is a registered trademark of Hewlett-Packard

HP-UX is a registered trademark of Hewlett-Packard

Pentium is a registered trademark of Intel Corporation

UNIX is a registered trademark of X/Open Company Limited

Limited Warranty

Lucent Technologies provides a limited warranty for this product. For more information, consult your local Account Representative.

Ordering information

The ordering number for this document is 190-224-158R8.0.

To order this document within the continental United States, call 1-888-LUCENT8 (1–888–582–3688).

To order this document outside the continental United States, call your Lucent customer team representative.

Support

Information product support

You may call the toll-free hotline at 1–866–LUCENT8 (1–866-582-3688) for customer assistance and troubleshooting 24 hours a day. See your Lucent Technologies account representative for further details.

Technical support

In the continental United States, when you need additional technical assistance, the Lucent Technologies Global TSS Contact Center is your first point of contact. Technical assistance is available 24 hours a day, 7 days a week. Contact the Global TSS Contact Center at 1–866–LUCENT8 (1–866-582-3688) .

Outside the continental United States, contact your Local Customer Support (LCS) or the support organization designated by your Lucent customer team representative. If you are unsure of who to call, contact the Global TSS Contact Center at 1–630–224–4672.

Contents

About this information product

1 The Basics

2 Security Management

3 System Administration for Standalone Configurations

4 Database Maintenance

5 Management Communication

List of Figures

7 Cluster Administration GUI Operations

List of Tables

2 Security Management

About this information product

Purpose

This preface provides an overview of this information product.

Reason for reissue

This ***Administration Guide*** is a revised document that supports the Navis™ Optical Element Management System (EMS), Release 8.0 (R8.0). The document has been reissued to describe new features for the Navis™ Optical EMS, R8.0.

Safety labels

Safety labels are not applicable to this document.

Intended audience

This guide explains to users how to administer the Navis™ Optical EMS. This guide is written primarily for operations personnel who are to administer the Navis™ Optical EMS.

How to use this information product

The following table describes the structure and content of each chapter in this guide.

Section	Title	Description
Preface	About This Information Product	Explains this document's purpose, its intended audience, and how to use it.
Chapter 1	Chapter 1, "The Basics"	Provides the basics about the Navis™ Optical EMS application and administration of the application
Chapter 2	Chapter 2, "Security Management"	Provides conceptual information about security and the tasks needed to control access to the Navis™ Optical EMS and its managed NEs
Chapter 3	Chapter 3, "System Administration for Standalone Configurations"	Provides the tasks needed to start up, shut down, and reboot the Navis™ Optical EMS application.
Chapter 4	Chapter 4, "Database Maintenance"	Provides the tasks needed to maintain the Navis™ Optical EMS database.
Chapter 5	Chapter 5, "Management Communication"	Provides the tasks needed to configure communication interfaces with NEs managed by the Navis™ Optical EMS.
Chapter 6	Chapter 6, "Trouble Clearing"	Explains the concepts and provides the tasks that are needed to facilitate troubleshooting problems with software components of Navis™ Optical EMS and its communications interfaces.
Chapter 7	Chapter 7, "Cluster Administration GUI Operations"	Describes the concepts of and provides the tasks that are needed to use the cluster administration GUI, which is a separate Navis™ Optical EMS GUI used to monitor redundant server operations.

Section	Title	Description
Appendix A	Appendix A, " Available Functions/T1 Commands"	Provides a list of the available functions/TL1 commands for each Authorization Level

Conventions used

This section provides information to assist users of this information product.

Commands to be input are shown in bold type.

Items shown in a command line in ***italics*** indicate the name of a directory/file or that this value is variable depending on the specific name of the data item, filename, or directory.

Related documentation

This information product is part of a set of documents that supports Navis™ Optical EMS.

List of documents

The document set that supports Navis™ Optical EMS includes:

- *Navis™ Optical EMS Maintenance Guide*— this document instructs users on how to maintain network elements managed by Navis™ Optical EMS.
- *Navis™ Optical EMS Administration Guide*—this document instructs users on how to administer Navis™ Optical EMS and the managed network elements.
- *Navis™ Optical EMS Provisioning Guide*—this document instructs users how to use the Navis™ Optical EMS to provision the managed network elements.
- *Navis™ Optical EMS Installation Guide*—this document instructs system administrators and other operations personnel how to install the Navis™ Optical EMS.
- *Navis™ Optical EMS Applications and Planning Guide*—this document provides users with information used to understand the applications for Navis™ Optical EMS, plan their use of the Navis™ Optical EMS, and understand what components must be ordered for the Navis™ Optical EMS application.
- *Navis™ Optical EMS Terminology Guide*—this document is a comprehensive glossary of terms and acronyms related to the Navis™ Optical EMS and its managed network elements.

On-line documentation

Online versions of the document set listed—except for the *Navis™ Optical EMS Terminology Guide*—are available through the Help menu option on the Map window main menu in the Navis™ Optical EMS Graphical User Interface (GUI).

On-line help

The Navis™ Optical EMS software includes on-line help for each window with a Help button. Each window has an associated help screen that describes the purpose of the window, basic window navigation, field descriptions, and button functions.

How to comment

To comment on this information product online, go to *http://www.lucent-info.com/comments* or email your comments to ctiphotline@lucent.com (mailto:ctiphotline@lucent.com).

Customer satisfaction is extremely important to Lucent Technologies. All users are encouraged to provide feedback on Navis™ Optical EMS information products.

How to order

To order Navis™ Optical EMS information products: contact Lucent Technologies:

From the United States, call 1-888-LUCENT8 (1-888-582-3688),
FAX: 1-800-566-9568

From Canada, North American Region call 1-317-322-6615, or e-mail: intlnaorders@lucent.com

From Europe, the Middle East, and Africa (EMEA), Asia, Pacific Region, and China, Caribbean, and Latin America (CALA), call 1-317-322-6416, or e-mail: intlorders@lucent.com

The worldwide fax number is 1-317-322-6699

1 The Basics

Overview

Purpose This chapter provides the basic information needed to administer the Navis™ Optical EMS application.

Contents

□

Product Basics

The product being administered

The Navis™ Optical EMS is an enhanced graphical tool and a general configuration management aid for Lucent's WaveStar® , Lambda™, and Metro™ product families. These product families consist of intelligent optical Network Elements (NEs) that can discover and report their configuration, including physical equipage and connectivity within the network. The Navis™ Optical EMS application enhances the capabilities of its supported NEs and optimizes the role of these NEs in management functions to create an intelligent operations environment.

For a list of supported NEs and the particular release of each NE that R8.0 of the Navis™ Optical EMS supports, refer to the ***Navis™ Optical EMS Applications and Planning Guide.***

Northbound and southbound interfaces

The Navis™ Optical EMS application provides two types of interfaces:

- ***Northbound interfaces*** enable the Navis™ Optical EMS application to communicate with other OSs, such as the Navis™ Optical Network Management System (NMS).
- ***Southbound interfaces*** enable the Navis™ Optical EMS application to communicate with its supported NEs.

For detailed explanation of these interfaces, refer to the ***Navis™ Optical EMS Applications and Planning Guide.***

The operating environment

The Navis™ Optical EMS application runs on a Hewlett-Packard® (HP®) L-class or N-class server running HP-UX® version 11.0. Associated peripherals (console, terminals, and printers) and desktops (PCs and/or workstations) are connected via an Ethernet LAN, with the option to interface via a Wide Area Network (WAN).

The HP servers can be configured as standalone servers with redundant components, which is referred to as ***basic host redundancy***, or as redundant systems in local or geographically dispersed locations, which is referred to as ***local redundancy*** or ***geographic redundancy.***

These redundancy configurations provide multiple levels of application and host redundancy for backup support and disaster recovery. The local and geographic redundancy configurations require two similarly equipped servers that operate in an active/standby arrangement. The two servers, which are linked via a TCP/IP WAN segment, rely on data replication to provide near real-time database synchronization of the standby server with the currently active server.

Under typical operating conditions, the application runs on the active server, which actively monitors all NEs in the management domain. The backup server, which is in a hot-standby state, maintains data connections to the network and uses data replication from the active server to keep its database current. If the primary server fails, administrator-initiated manual switchovers can prevail.

The Navis™ Optical EMS GUI, which is a common interface to all supported NEs, provides graphical features such as multilevel displays of the network, an automatically generated map of the overall managed domain, hierarchically arranged equipment displays down to the shelf level, a graphical representation of the cross connection configuration with point and click provisioning, and form and menu-based provisioning for viewing and setting provisional parameters. The GUI also supports a cut-through feature that enables TL1 commands to be input directly to supported NEs and it supports numerous custom-tailored options so users can create displays that suit their preferences.

For detailed a explanation of this operating environment, refer to the ***Navis™ Optical EMS Applications and Planning Guide.***

□

Administration Basics

Administration Definition

The administration of the Navis™ Optical EMS application involves the management and maintenance of the application, its hardware, and its users.

Administration levels

Administrative tasks are performed on the following levels:

- On the ***system*** level, the administrator performs tasks that are directly related to the Navis™ Optical EMS application and the hardware components on which the application runs and the software components on which the application relies.
- On the ***network*** level, the administrator performs tasks that are directly related to LAN/WAN connections, and the connections of individual machines and the interconnections among machines.
- On the ***internetwork*** level, the administrator performs tasks that are directly related to the interworking of the Navis™ Optical EMS application with its managed NEs.

Administrator responsibilities

The administrator's responsibilities are grouped into the following categories:

- ***Security Management***, which includes user ID and password administration for the application and the supported NEs, global password administration, and the assignment of users into command and target groups.
- ***System Administration***, which includes bringing the servers up and down, rebooting the application, and installing software.
- ***Database Maintenance***, which includes doing a partial or total backup and restoration of the application database, and importing and exporting the application database to tapes or directories.
- ***Management Communication***, which includes configuring and/or setting up communications protocols on the supported NEs.
- ***Trouble Clearing***, which includes troubleshooting problems dealing with the software components of the application and its communication interfaces.
- ***Cluster GUI Administration***, which involves bring up the cluster administration GUI on redundant systems, e-mail administration, and manual switchovers of servers.

□

Lucent Technologies
Bell Labs Innovations

2 Security Management

Overview

Purpose

This chapter provides general information about controlling access to the Navis™ Optical EMS application and its managed network elements (NEs) and explains the concepts of password administration and the various aspects of network security. In addition, this chapter provides the procedures that must be performed to control access to Navis™ Optical EMS and its managed NEs.

The Navis™ Optical EMS application provides network security by allowing the administrator to define users and the extent of their access to NEs in the network and their ability to perform certain system functions and commands.

Levels of access are defined by:

- User ID and user password administration
- NE login administration and NE command access
- Command Groups
- Target Groups

Before you begin

Read the concepts explained in the beginning of this chapter to understand the Security Management features that the application provides.

Contents

□

The User ID and User Password

Overview

In the Navis™ Optical EMS application, the user is identified by a login and password, and the system administrator grants access to that user to appropriate system functions and features.

User logins

A user login is created for each user who accesses the system. The user ID assigned to each user login must be a unique, 2 to 10 character alphanumeric string, without white spaces. Special characters, such as ; * & and @ are not allowed.

When a user logs into application, the user ID is validated with the current password. If a user fails to log in with a valid user ID/password combination after a number of times (which is administrator defined), the user ID is automatically disabled and the user cannot log into the application. An `Invalid Login` message is displayed, an alarm is issued, and the user ID session is terminated.

When creating (adding) a user ID, the administrator must also define the NEs that can be accessed using this login and the commands that can be issued to the accessible NEs. For each user ID, the administrator must select the ***Target Group***, which determines the NEs that can be accessed using the user ID, and the ***Command Group***, which determines the Authorization level and types of commands that can be issued to the accessible NEs, as defined by the Target Group for the user ID.

The following table shows the default value with which a user login is initially created.

Table 2-1 Initial Default Values when Creating User Logins

Field	Default Value
User ID Login Type	GUI
Password	No default password exists; administrator must enter
Command Group	Empty
Target Group	Empty

In addition, the administrator can copy the login group, Command Group, and Target Group settings from an existing user to a newly defined one.

Changing a user login

To change a user's login, the system administrator must first delete the user and then re-enter the user in the system with a new login.

User passwords

The Change Password function is the only administration function that is available to the Navis™ Optical EMS application user. A user password can be changed at any time. The system verifies that the old password entered matches the one stored in its database for the user.

The first time a user ID (login) is used to log into the Navis™ Optical EMS application, the application forces the default password to be changed to a new password, and displays the Change Password window.

Passwords must be changed after a certain period of time (as defined by the system administrator via the Global Security Provisioning window). If a password is about to expire, and a user attempts to log into the system, a pop-up window advises that the password is about to expire and allows the user to change the password. If the expiration period is reached, and the user does not change the password before attempting to log into the application, system access is denied.

The Navis™ Optical EMS application maintains a history of password usage. If a user attempts to change the password to one previously used, the application advises that a different password must be specified.

Valid user password format

A valid user password consists of from 6 to 10 characters. A password must include at least two alphabetic characters, at least one numeric, and at least one special character (!#$%^&*()-+_=?). The following special characters are not permitted (:,;).

A new password must differ from the old one by at least three characters. An uppercase letter and its corresponding lowercase equivalent are treated as identical, which means that the new password must contain at least three new and different characters that were not present in the old password.

Example: The password ***ems+123*** can be changed to ***abc+123*** because the characters ***a***, ***b***, and ***c*** were not present in the old password. The password ***ems+123*** cannot be changed to ***ems+321*** because new characters have not been introduced in the new password.

The new password cannot contain the user ID as part of the password.

Example: The user login ***john*** cannot have the password ***john+123***.

User passwords and the Global Security Provisioning feature

The Global Security Provisioning feature in Navis™ Optical EMS application allows the application administrator to set up the system to ***remember*** and prohibit a user from using a specific number of previous passwords. The default number of previous passwords that the application recalls and prevents from re-use is five. The administration can disable this parameter by setting the value to zero (0) so the system does not recall any previous passwords.

User management

The Navis™ Optical EMS application has built-in security features to inhibit or prevent unauthorized user access to the system and to monitor user activity.

Through GUI functions, the application administrator or a user with a privileged login can:

- terminate an active user login's session
- enable or disable user logins
- set a limit of the number of failed login attempts before preventing a user from logging into the Navis™ Optical EMS
- set the password aging interval for user logins
- issue a warning notice to users when their password is about to expire
- maintain a history of previously used passwords
- set the session timeout interval for logins
- set the expiration period for user logins
- specify the message that is issued when a user successfully logins into Navis™ Optical EMS
- view all currently active user login sessions

Alarms and user logins and user passwords

The application generates a Minor alarm, which can indicate a possible threat or attempted breach of system security, when any of these conditions occur:

- a user ID is automatically disabled due to excessive failed login attempts
- a user ID is deleted due to lack of use
- a password change for a user ID is unsuccessful

Only the application administrator can access a Minor alarm, which is generated against the application itself (TID=EMS).

□

Global Password Administration

Overview

The Navis™ Optical EMS GUI, which is available only for Lucent Technologies NEs, enables the primary and/or backup passwords to be changed for a number of NEs at the same time.

This feature allows a global password change for the following:

- individual NEs by TID
- all NEs
- NEs by type
- aggregates, which are a collection of NEs

Changes to the primary and/or backup NE passwords are sent to the selected NE(s) and the local Navis™ Optical EMS database is automatically updated with the password information.

The global password update process can be aborted at any time while the Global Password Administration window is open.

Only one person can use the Global Password Administration feature at a time.

NE default login/password

NEs have default logins/passwords that are manufacturer defined prior to shipment. The Navis™ Optical EMS user requires an NE login and NE password to gain access to the NE. The system GUI allows you to modify an individual NE’s primary and backup password through the Add/Modify an NE window or via cut-through mode. However, if the network has numerous NEs, this process can be time-consuming.

Password aging on the WaveStar® BWM and the WaveStar® TDM 10G (STM-64)

The WaveStar® BWM and the WaveStar® TDM 10G (STM-64) NEs have a password aging feature for security reasons. When a software upgrade is performed for either NE, one of the default NE passwords used to log into the NE to perform the upgrade automatically expires upon first use, and must be changed using the CIT. The Navis™ Optical EMS uses these default NE passwords to log into the NE and to obtain information during the subnetwork autodiscovery process. The default NE passwords changed using the CIT during the software upgrade may not be known by the Navis™ Optical EMS. However, as long as the second default NE password remains the same, the Navis™ Optical EMS can use it to log into the NE during subnetwork autodiscovery.

Once the Navis™ Optical EMS has been able to log into a WaveStar® BWM or WaveStar® TDM 10G NE using the unchanged default NE password, use the "Globally Administer NE Passwords" (2-18) task to manually change the NE password of the superuser login that was changed using the CIT during installation. Then, the Navis™ Optical EMS has access to both Super User NE logins/passwords to log into the WaveStar® BWM and WaveStar® TDM 10G NEs.

If one or both passwords that the Navis™ Optical EMS used to successfully log into a WaveStar® BWM or WaveStar® TDM 10G NE expire, Navis™ Optical EMS issues an `ed-PID` command to change the passwords of the NE Super User logins to ***SNC+01*** and ***WBM+01***.

The password aging feature for the WaveStar® BWM and WaveStar® TDM 10G NEs can be turned off via the CIT or by issuing the appropriate TL1 command through the Navis™ Optical EMS cut-through feature. See the NE documentation for appropriate TL1 command.

The new passwords are updated in the Navis™ Optical EMS database of the current host after they are changed. Any additional EMS hosts or CIT interfaces have to be updated with the new passwords as well to enable logging into the affected NEs.

□

NE Logins and Passwords

Overview

The Navis™ Optical EMS application allows an administrator or a user with a privileged login to administer user logins that are used to log directly into an NE. The level of NE access and the type of activities available to an NE login can be defined.

The application allows the administrator to do the following:

- define NE logins
- define passwords for NE logins
- define User Privilege Codes (UPCs), which are a listing of exact permission levels to access a specific NE function
- define, temporary NE logins with an expiration date, for some types of NEs
- copy UPC settings from another login, which ***does not*** include the ability to copy the login or password from another NE login
- define the Password Aging/Expiration Time, which includes the length of time (in days) that a password for an NE login can be used before it has to be changed
- define the User ID Status, which can be specified as Active or Suspended (some NE types)
- define the Inactivity Timeout, which sets the timer for session inactivity before the system automatically times out
- define Priority, for some NE types, which sets the priority for logins

Format of NE logins and NE passwords

The NE login is a 1 to 20 character alphanumeric string

The NE password must adhere to this format:

- It must be a 6 to 10 character alphanumeric string.
- One character must be one of these special characters # , % , or +
- The password must begin with a letter.

UPCs A User Privilege Code (UPC) is a combination of a Function Category and an Authorization Level. The administrator relies on a UPC to indicate the level of access that a user has to NE functions when adding or modifying an NE login or copying another NE login's settings. The Functional Categories are as follows:

Table 2-2 Functional Categories of UPCs

Functional Category Name	The Functional Category contains all...	This Functional Category applies to the...
Maintenance (M)	fault management-related functions/features	WaveStar® BWM, WaveStar® 2.5G (OC-48 2F), WaveStar® 10G (OC-192 2F), WaveStar® 10G (STM-64),WaveStar® OLS 1.6T, all Lambda NEs, and all Metropolis™ NEs
Provision (P)	configuration management-related functions/features	WaveStar® BWM, WaveStar® 2.5G (OC-48 2F), WaveStar® 10G (OC-192 2F), WaveStar® 10G (STM-64),WaveStar® OLS 1.6T, all Lambda NEs
Performance Management (PM)	performance management-related functions/features	WaveStar® BWM, WaveStar® 2.5G (OC-48 2F), WaveStar® 10G (OC-192 2F), WaveStar® 10G (STM-64),WaveStar® OLS 1.6T
Security (S)	EMS security and administration-related functions/features	WaveStar® BWM, WaveStar® 2.5G (OC-48 2F), WaveStar® 10G (OC-192 2F), WaveStar® 10G (STM-64),WaveStar® OLS 1.6T, all Lambda NEs
Debug (D)	debugging related functions/features	WaveStar® BWM, WaveStar® 2.5G (OC-48 2F), WaveStar® 10G (OC-192 2F), WaveStar® 10G (STM-64)

Table 2-2 Functional Categories of UPCs (continued)

Functional Category Name	The Functional Category contains all...	This Functional Category applies to the...
Test Access (TA)	test-access related functions/features	WaveStar® BWM only
Privileged	potentially service affecting user functions	all Metropolis™ NEs only
General	non-service affecting provisioning and maintenance functions	all Metropolis™ NEs only
Reports Only	retrieve commands and/or functions only	all Metropolis™ NEs only
All	Maintenance, Provisioning, Performance Management, Security, and Test Access functions/features	all Metropolis™ NEs only

Each Functional Category, which can contain the ***TL1 commands*** and/or the actual ***functions*** that a user can perform, has Authorization Levels that are consistent with the NE privileges that are allowed for the particular level. Refer to Appendix A, " Available Functions/T1 Commands" for a list of TL1 Commands and/or Functions that are available for each Authorization Level. The Authorization Levels are as follows:

Table 2-3 Authorization Levels for Functions/TL1 Commands

Authorization Level	For actual Functions to be performed...	For TL1 Command to be issued...
1 (lowest level)	Empty	Minimal

Table 2-3 Authorization Levels for Functions/TL1 Commands (continued)

Authorization Level	For actual Functions to be performed...	For TL1 Command to be issued...
2	Reports Only	Reports Only, which is merged with Level 1 to be retrieve only.
3	General	General, which includes provisioning and maintenance functions that are not service affecting.
4	Privileged	Privileged, which includes functions that are potentially service affecting.
5 (highest level)	Superuser*	Superuser, which includes user login specifications.
* The UPC for an NE superuser login cannot be modified. Each NE must have at least one NE login with superuser authorization to support any management task that might be required for the NE.		

UPC Examples

The combination of a Functional Category and Authorization Level constitutes a User Privilege Code (UPC) for a specific set of features.

Example: A UPC of ***M3*** indicates that a Navis™ Optical EMS user login can execute all Maintenance Category functions with Authorization Level 3 or less. The user logging into an NE with this UPC has access to these EMS ***features***:

- Cut-Through
- TL1 Macro Builder
- TL1 Broadcaster
- View Alarm Monitoring Statistics
- View Alarm Severity Assignment Profiles
- Re-synchronize Alarms
- View Protection Switch Messages
- Provision Alarm Provisioning

Example: A UPC of ***PM3*** indicates that a user ID and/or a user login can execute all Performance Management functions with Authorization Level 3 or less. The ***TL1 commands*** that a user ID and/or a user login with this UPC would be authorized to issue are the following:

- `ACT-USER`
- `CANC-USER`
- `RTRV-TCA-ASGNMT`
- `RTRV-TCA-PROF`
- `RTRV-PM-rr`; where: `rr` equals OC-48, OC-12, OC-3, EC1, STS1, or T3
- `INIT-REG`

The respective NE documentation explains which TL1 commands can be issued for each Functional Category/Authorization Level.

□

Command Groups

Definition

A Command Group, also known as a ***user class***, is a collection of Navis™ Optical EMS and NE commands that a specified user is allowed to enter through the system GUI. When a user login is created, each user is assigned to one and only one Command Group.

Both the Target Group and the Command Group that a user can access are specified when the user login is created.

Creation of Command Groups

The Navis™ Optical EMS application is initially set up with ***predefined*** Command Groups. The administrator can also create Command Groups to suit the needs of the installation, which are referred to as ***user-defined*** command groups. When creating a Command Group, a set of commands from an existing command group can be copied into the new group. Command Groups can also be modified or deleted.

The application allows a maximum of 100 predefined and user-defined Command Groups.

Predefined Command Groups

Each predefined Command Group allows a set of TL1 commands to be issued that correspond to certain User Privilege Code (UPC) levels.

The following list of all predefined NE Command Groups with UPCs shows the level of TL1 commands that can be issued.

Table 2-4 Predefined NE Command Groups and UPCs

Command Group Name	Description	User Privilege Codes
Empty	Set up without any commands.	M1, P1, PM1, S1, T1
Maintenance	Allows access to all Maintenance and Performance Management Category commands with Authorization Level 4 or less. Allows user to view and modify all NE Maintenance information.	M4, P3, PM4, S1, T4

Table 2-4 Predefined NE Command Groups and UPCs (continued)

Command Group Name	Description	User Privilege Codes
Provisioning	Allows access to all Provisioning Category command with Authorization Level 4 or less. Allows user to view and modify all NE provisioning information.	M1, P4, PM1, S1, T1
Reports Only	Allows access to all categories of commands with Authorization Level 2 or less. Restricts user to view NE information, but not change it.	M2, P2, PM2, S2, T2
General	Allows access to all categories of commands with Authorization Level 3 or less. Allows a user to view and modify most NE information.	M3, P3, PM3, S3, T3
Privileged	Allows user access to all categories of commands with Authorization Level 4 or less. Allows a user to view and modify most NE information, except Administrator functions.	M4, P4, PM4, S4, T4
All	Allows access to all commands, including administrator functions supported by the NE. Is the superuser NE Command Group and is automatically assigned to the ***admin*** logins; other user IDs can be assigned to ***all***. Usually reserved for the EMS administrator.	M5, P5, PM5, S5, T5

System administrator functions

The Navis™ Optical EMS system administrator can do the following:

- add, modify, or delete Command Groups
- define additional Command Groups as needed
- copy the contents of an existing Command Group to a newly defined Command Group

□

Target Groups

Definition

A Target Group is a collection of NEs to which a user has access and can execute commands. A user is assigned to one and only one Target Group and can only access the NEs in this Target Group. Along with Command Groups, Target Groups define user permissions and provide network security.

Both the Target Group and the Command Group that a user can access are specified when the user login is created.

Creation of Target Groups

The Navis™ Optical EMS application is initially set up with two ***predefined*** with Target Groups:

- ***all targets***, which provides access to all NEs in the network
- ***empty***, which denies access to any NEs

The administrator or a user with a privileged login can also create Target Groups to suit the needs of the installation, which are referred to as ***user-defined*** Target Groups. When creating a Target Group, a set of commands from an existing Target Group can be copied into the new group. Target Groups can also be modified or deleted.

The application allows a maximum of 100 predefined and user-defined Target Groups.

System administrator functions

The Navis™ Optical EMS system administrator can do the following:

- add, modify, or delete Target Groups
- define additional Target Groups as needed
- copy the contents of an existing Target Group to a newly defined Target Group

□

Change the User Password

Purpose Use this procedure to change the user password.

Before you begin Read the conceptual information about user passwords in the "The User ID and User Password" (2-3) section.

Related tasks See "Target Groups" (2-15), "Modify a User" (2-24), and "Globally Provision User Login/Password Parameters (Global Security Provisioning Feature)" (2-55).

Task Complete the following steps to change your user password.

1 Select **Administration** from the main menu of the Map window.

Result:

A sub-menu appears.

2 Choose **Security** from the displayed sub-menu.

Result:

A sub-menu appears.

3 Choose **Change EMS Password** from the Security menu.

Result:

The Change Password window is displayed.

4 Type your current password into the Old Password field.

5 Type your new password into the New Password field.

6 Type the same new password into the Confirm New Password field.

Result:

If the system does not issue any warning messages and the password is valid, go to step 8.

If the system issues a warning message that the new password entered is invalid, go to step 7.

If the **previous password** option in the Global Security Provisioning window is enabled and the system warns that you have changed the password to one that was previously used, go to step 7.

7 If the new password that was entered is still invalid, retype another new, valid password.

8 Select **OK** to enter the password change into the system.

END OF STEPS

□

Globally Administer NE Passwords

Purpose

Use this procedure to change the primary and/or secondary passwords for selected NE(s)/aggregate(s).

Before you begin

Make sure that you really want to proceed with changing the primary/secondary passwords.

You must be logged into the Navis™ Optical EMS application.

The NE(s) or aggregate(s) for which you are changing passwords must already exist in the application database.

If passwords are being changed for 20 or more NEs at a time, system performance might degrade.

Only one user can use the Global Administer NE Password function at a time.

Any changes made to the primary/secondary passwords for NEs will affect logging into the NEs from all EMS and CIT interfaces.

The WaveStar® BWM and the WaveStar® TDM 10G (STM-64) NEs have a password aging feature for security reasons. See "Global Password Administration" (2-6) for more information.

Task

Complete the following steps to change the primary and/or secondary passwords for the selected NE(s)/aggregate(s).

1 Access the Map window.

2 Select one or more NEs and/or aggregates on the Map window pane or subnetwork explorer, if you know for which NEs you want to perform this function.

OR

Select no NEs and/or aggregates at this point.

3 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

4 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

5 Select **Global Password Administration** from the Security sub-menu.

Result:

The Global Password Administration window is displayed.

6

TO CHANGE THE PASSWORD FOR...	CLICK THE...
one or more NEs	Show NEs radio button.
one or more aggregates	Show Aggregates radio button.
a specific NE of the same type	List by Type radio button. Click the down arrow for this field to display a list of NE types, then select the NE type.

7 Select the NE(s) or aggregate(s) for which the password(s) will be changed, from the Network Elements/Aggregates list. Use the arrow push buttons to move NEs/aggregates back and forth between the two lists, as needed.

Result:

When you select an NE or aggregate, the item moves from the Network Elements/Aggregates List to the Chosen NEs list.

8 Enter the new Primary Password for the selected NE(s)/aggregate(s) in the Primary Password field.

9 Re-enter the new Primary Password in the Re-enter Primary Password field.

10 If desired, enter a new Secondary Password in the Secondary Password field.

11 If a new Secondary Password has been entered, re-enter it in the Re-enter Secondary Password field.

12 To abort the password change operation while it is in progress, click the Abort button.

To initiate the password change(s), click the Apply button.

To close the window, click the Close button.

Result:

A Log Browser window is displayed, showing the status of the operation. This window remains open until you close it.

If the number of NEs selected is 20 or more, a pop-up message window appears, advising you that the EMS performance may be impacted and asking if you want to continue with the operation. Go to the next step.

13 If the number of NEs selected was more than 20 and the pop-up message did appear, choose `Y` to continue with the operation or `N` to cancel the operation.

END OF STEPS

□

Add a User

Purpose

Use this procedure to add a user's login and access permissions for Navis™ Optical EMS application. A unique user ID (login) must be defined for each user who accesses the application.

Before you begin

You must select the Target Group, which determines the NEs that can be accessed using this user ID, and the Command Group, which determines the Authorization level and types of commands that can be issued to the accessible NEs, as defined by the Target Group for this user login. Read the "The User ID and User Password" (2-3) section.

Related information

See "Add a Target Group" (2-33) and "Add a Command Group" (2-27).

Task

Complete the following steps to add a user login.

1 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

2 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

3 Select **User Provisioning** from the Security sub-menu.

Result:

The Manage Users window is displayed, showing the current list of user logins.

4 Click the Add button.

Result:

The Add a User window is displayed.

5 Fill in the following fields, as needed:

- Name—This is the user login field. A user login must be unique and contain from 2 to 10 alphanumeric characters with no white spaces. Uppercase and lowercase letters are allowed. No special characters are allowed. Spaces are not allowed. This field is required.
- Alias—This is an alternate label for the user. A user alias can be from 1 to 20 alphanumeric characters, in any combination. Uppercase and lowercase letters are allowed. Spaces are allowed. This field is required.
- Password—This is the user's password. A user password can be from 6 to 10 characters. The password must contain at least two alphabetic characters, at least one numeric character, and one special character (!#$%^&*()-+_=?). The following special characters are not permitted (:,;). This field is required.
- Confirm Password—This field is to confirm the user's password. If the entry in this field is not identical to the password entered in the Password field, a pop-up window is displayed with a warning message when the OK button is clicked. This field is required.
- Copy this user's settings—This field is used to copy another user's Login Type, Command Group, and Target Group settings. Click the down arrow to the right of the field to display a list of users. Select a user login from which to apply settings and then click the Load Settings button. This field is optional, and settings can be modified after these fields have been populated. ***Note: this function does not copy a user's preferences for Map display settings.***
- Login Type—This field is used to specify the type of login. The types are:
  - GUI—This user ID category is only allowed to access the EMS via the GUI client. Default Command Group = Empty, Default Target Group = Empty
  - ITM-NM—This user ID category is reserved for the interface between the Navis™ Optical EMS and Navis™ Optical NMS. Default Command Group = ALL. Default Target Group = ALL. The pre-defined user ID ***itm*** is defined as Navis™ Optical NMS.

  - NMS—This user ID category is reserved for the interface between the EMS and a generic Network Management System (NMS). Both Fault and Configuration Management functionality are available to this type of user ID. Default Command Group = Privileged, Default Target Group = ALL. The pre-defined user ID ***nms*** is defined as NMS.
  - ADMIN—This user ID category is reserved for the EMS system administrator. Default Command Group = ALL. Default Target Group = ALL. The pre-defined user ID ***admin*** is defined as ADMIN.

  Click the down arrow to the right of the field to display the choices. Select a login type. This field is required.

- Command Group—This field is used to specify which Command Group the user can access. Click the down arrow to the right of the field to display a list of choices. The choices are: Empty or a specific Command Group. Select a Command Group for user access. This field is required.
- Target Group—This field is used to specify which Target Group the user can access. Click the down arrow to the right of the field to display a list of choices. The choices are: Empty or a specific Target Group. Select a Target Group for user access. This field is required.

6 Click the OK button.

Result:

The Status Dialog window is displayed, indicating that the user is being added to Navis™ Optical EMS.

END OF STEPS

□

Modify a User

Purpose Use this procedure to change the attributes of a user login.

Before you begin You must create a user login.

The Login Type, Alias, Password, Command Group, and/or Target Group can be changed.

You cannot modify the attributes of predefined user IDs. Only the password of a predefined user ID can be changed.

Read all conceptual information provided in "The User ID and User Password" (2-3) section.

Related tasks See "Change the User Password" (2-16) and "Globally Provision User Login/Password Parameters (Global Security Provisioning Feature)" (2-55).

Task Complete the following steps to modify a user login's attributes.

1 Access the Map window.

2 Select **Administration** from the main menu bar on the Map window. .

Result:

The Administration menu is displayed.

3 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

4 Select **User Provisioning** from the Security sub-menu.

Result:

The Manage Users window is displayed, showing the current list of user logins.

5 Select a user login from the list.

6 Click the Modify button.

Result:

The Modify User window is displayed.

7 Change the Login Type, Password, Alias, Command Group, and/or Target Group fields as required.

8 Click the OK button.

Result:

The Status Dialog window is displayed, indicating that the changes to the user login are being made by the system.

END OF STEPS

□

Delete a User

Purpose Use this procedure to delete a user login from Navis™ Optical EMS.

Before you begin The TL1 Macro Builder Files created by a user must remain in the Navis™ Optical EMS database. These files must be removed either by the owner of the files (the user) or the system administrator.

Task Complete the following steps to delete a user.

1 Access the Map window.

2 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

3 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

4 Select **User Provisioning** from the Security sub-menu.

Result:

The Manage Users window is displayed.

5 Select the user to be deleted from the list of user logins.

6 Click the Delete button.

Result:

A pop-up window is displayed, asking if you really want to delete the user.

7 Select **Yes** to delete the user.

END OF STEPS

□

Add a Command Group

Purpose Use this procedure to add a Command Group.

Before you begin Read the conceptual information in the “Command Groups” (2-13) section.

Related information See “Add a User” (2-21) and “Add a Target Group” (2-33).

Task Complete the following steps to add a Command Group.

1 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

2 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

3 Select **Command Groups** from the Security sub-menu.

Result:

The Manage Command Groups window is displayed, showing the current list of Command Groups.

4 Click the Add button.

Result:

The Add a Command Group window is displayed.

5 Fill in the following fields, as needed:

- Command Group Name—This is the Command Group name. A Command Group name cannot contain spaces. This field is required.
- Command Group Alias—This is the Command Group alias (alternate label). This field is required.
- Copy settings from this group—This field is used to copy a set of commands from an existing Command Group into the new one. Click the down arrow to the right of the field to display a list of Command Groups. Select a Command Group from which to copy a set of commands and then click the Load Settings button. This field is optional, and the contents of the EMS and NE Command fields can be modified after this information has been copied.

Important! If you provide an invalid Command Group name or alias, the system informs you with a warning message.

6 Use the push buttons to move commands from the list of available commands in the EMS Commands scroll list to the EMS Commands in This Group list, as needed.

7 Use the push buttons to move commands from the list of available NE commands in the Network Elements Commands scroll list to the NE Commands In This Group list, as needed.

8 Click the Apply button to activate your choices, or click the OK button to activate your choices and close the window.

Result:

The Status window is displayed, indicating the Command Group is being added to Navis™ Optical EMS.

9 Click the Close button to close the Status window and return to the Map window.

END OF STEPS

□

Modify a Command Group

Purpose

Use this procedure to change a Command Group once it has been created.

Before you begin

Read the conceptual information in the “Command Groups” (2-13) section.

The Command Group name or alias cannot be modified.

Task

Complete the following steps to modify a Command Group.

1 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

2 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

3 Select **Command Groups** from the Security sub-menu.

Result:

The Manage Command Groups window is displayed, showing the current list of Command Groups.

4 Select the Command Group to be modified from the list.

5 Click the Modify button.

Result:

The Modify Command Group window is displayed.

6 Change the Copy From Group, EMS Command List, or NE Command List as desired.

7 Click the OK button.

Result:

The Status window is displayed, indicating that the changes to the Command Group are being made by Navis™ Optical EMS.

8 Click the Close button to close the Status window and return to the Map window.

END OF STEPS

□

Delete a Command Group

Purpose Use this procedure to delete a Command Group from the Navis™ Optical EMS.

Before you begin Read the conceptual information in the "Command Groups" (2-13) section.

Users assigned to the Command Group to be deleted must first be reassigned to another Command Group. The reassignment is done as part of this task.

Task Complete the following steps to delete a Command Group.

1 Access the Map window.

2 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

3 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

4 Select **Command Groups** from the Security sub-menu.

Result:

The Manage Command Groups window is displayed, showing the current list of Command Groups.

5 Select the Command Group to be deleted from the list.

6 Click the Delete button.

7 The Reassign Users to Command Group window is displayed if any users are assigned to the Command Group.

8 Choose a Command Group from the list to which you want to reassign all users of the Command Group being deleted.

9 Click the OK button.

Result:

The Command Group is deleted.

END OF STEPS

□

Add a Target Group

Purpose Use this procedure to add a Target Group.

Before you begin Read the conceptual information in the “Target Groups” (2-15) section.

Related information See “Add a User” (2-21) and “Add a Command Group” (2-27).

Task Complete the following steps to add a Target Group.

1 Access the Map window.

2 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

3 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

4 Select **Target Groups** from the Security sub-menu.

Result:

The Manage Target Groups window is displayed, showing the current list of Target Groups.

5 Click the Add button.

Result:

The Add a Target Group window is displayed.

6 Fill in the following fields, as needed:

- Target Group Name—This is the Target Group name. A Target Group name cannot contain spaces. This field is required.
- Target Group Alias—This is the Target Group alias (alternate label). This field is required.
- Copy settings from this group—This field is used to copy a set of NEs from an existing Target Group into the new one. Click the down arrow to the right of the field to display a list of Target Groups. Select a Target Group from which to copy a set of NEs and then click the Load Settings button. This field is optional, and the contents of the Target Group can be modified after this information is copied.

Important! If you provide an invalid Target Group name or alias, the system informs you with an error message.

7 Use the push buttons to move NEs from the Network Element list scroll list to the NEs in This Group list, as needed.

8 Click the OK button.

Result:

The Status window is displayed, indicating that the Target Group is being added to Navis™ Optical EMS.

9 Click the Close button to close the Status window and return to the Map window.

END OF STEPS

□

Modify a Target Group

Purpose

Use this procedure to change a Target Group once it has been created.

Before you begin

Read the conceptual information in the "Target Groups" (2-15) section.

The Target Group name or alias cannot be modified. Certain Target Groups cannot be modified or deleted; this is indicated on the Target Group Manager window.

Task

Complete the following steps to modify a Target Group.

1 Access the Map window.

2 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

3 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

4 Select **Target Groups** from the Security sub-menu.

Result:

The Manage Target Groups window is displayed, showing the current list of Target Groups.

5 Select the Target Group to be modified from the list.

6 Click the Modify button.

Result:

The Modify Target Group window is displayed.

7 Change the Copy From Group, and/or NEs in This Group fields, as desired.

8 Click the OK button.

Result:

The Status Dialog window is displayed, indicating that the changes to the Target Group are being made by Navis™ Optical EMS.

END OF STEPS

□

Delete a Target Group

Purpose Use this procedure to delete a Target Group from Navis™ Optical EMS.

Before you begin Read the conceptual information in the “Target Groups” (2-15) section.

Users of the Target Group to be deleted must first be reassigned to another Target Group. The reassignment is done as part of this task. Certain Target Groups cannot be modified or deleted; this is indicated on the Target Groups Manager window.

Task Complete the following steps to delete a Target Group.

1 Access the Map window.

2 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

3 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

4 Select **Target Groups** from the Security sub-menu.

Result:

The Manage Target Groups window is displayed, showing the current list of Target Groups.

5 Select the Target Group to be deleted from the list.

6 Click the Delete button.

7 The Reassign Users to Target Group window is displayed if any users are assigned to the Target Group.

8 Choose a Target Group from the list to which you want to reassign all users of the Target Group being deleted.

9 Click the OK button.

Result:

The Target Group is deleted.

END OF STEPS

□

Add an NE Login

Purpose Use this procedure to add an NE login.

Before you begin Read the conceptual information in the "NE Logins and Passwords" (2-8) section.

The NE(s) to which you want to add the NE login must exist in the Navis™ Optical EMS database.

In step 2, you will have to select an NE on the Map window. For instructions on selecting an NE, see the procedure "Select/Deselect NEs or Aggregates on the Map Pane" (2-61).

Task Complete the following steps to add an NE login to an NE.

1 Access the Map window.

2 Select an NE on the Map window.

OR

Select no NE at this point.

3 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

4 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

5 Select **NE Login Administration** from the Security sub-menu.

If you did not choose an NE in step 2, the Choose an NE window is displayed. Choose an NE from the list by double-clicking on the NE's TID. The chosen NE is highlighted. Click the OK button.

Result:

The Manage NE Login window for the chosen NE is displayed, showing the current list of NE logins.

6 Click the Add button.

Result:

The Add login window for the chosen NE is displayed.

7 Fill in the following fields, as needed:

- Login—This is the NE login. Up to 20 characters are allowed. This field is required.
- Password—This is the NE login's password. An NE password must be 6 to 10 alphanumeric characters, with at least two non-alphabetic characters, of which one character must be one of the following special characters (# % +). The password must begin with a letter. This field is required.
- Copy this user's settings—click the down arrow next to this field to display a list of NE logins from any applicable NE from which to copy login settings; in other words, the User Privilege Code(s) that define the level of NE access for the selected NE login. To load/display the User Privilege Codes for the NE login to be copied from, click the Load Settings button directly below the Copy this user's settings field. This field is optional. ***Note: this function does not copy another login or password, which cannot be copied from another user***.
- Login Type: (Check the Box, if this User is a Temporary User)—Click on this box to place a check in it if the NE login being created is for a temporary user. This field is optional. If this option is selected, enter a date (in MM-DD-YYYY format) in the User ID Expiration Date field.***Note: Some NEs do not have the Login Type field activated.***
- User Privilege Code—This is the User Privilege Code field. Enter one or more User Privilege Codes to specify the level of NE access for this NE login. Some NE types require you to enter an ampersand (&) between each User Privilege Code when entering more than one. Values for User Privilege Codes vary by NE type.

- Inactivity Timeout (some NE types)—This is the inactivity timer for an NE login session. This field is optional.
- Password will expire after (days)—This field specifies the number of days in which a password is to expire.
- Priority (some NE types)—This is the order (priority) for NE logins. The default is 1. This field is optional.
- Passwords will expire after—This is the Password Aging field. Click the up and down arrows on this spinner field to select the number of days after which the specified password will expire. The default is 90 days. If you select 0 or leave the value at 0, the password will not expire for this NE login. This field is required.

8 Click the Apply or OK button to activate your choices.

A status dialog window is displayed, indicating that the NE login request is being processed. When it is finished, the NE login has been added.

END OF STEPS

□

Modify an NE Login

Purpose

Use this procedure to modify the attributes of an NE login. If the same NE login is used for more than one NE, the same changes can be made for every NE using that login.

Before you begin

Read the conceptual information in the "NE Logins and Passwords" (2-8) section.

In step 2, you will have to select an NE. For instructions, see "Select/Deselect NEs or Aggregates on the Map Pane" (2-61).

Task

Complete the following steps to modify an NE login for an NE.

1 Select an NE on the Map window.

OR

Select no NE at this point.

2 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

3 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

4 Select **NE Login Administration** from the Security sub-menu.

If you did not choose an NE in Step 1, the Choose an NE window is displayed. Choose an NE from the list by double-clicking on the NE's TID. The chosen NE is highlighted. Click the OK button.

The Manage NE Login window for the chosen NE is displayed, showing the current list of NE logins.

Result:

The Manage NE Login window for the chosen NE is displayed, showing the current list of NE logins.

5 Select the NE login to be modified from the list of NE logins.

6 Click the Modify button.

Result:

The Modify window for the chosen NE login is displayed.

7 Change the Password, Password Aging, Copy this user’s settings, Login Type (if applicable), User ID Expiration Date (for the Login Type field), and User Privilege Code fields as desired.

8 Click the OK or Apply button to activate your choices.

Result:

A status dialog window is displayed, indicating that your modifications are being processed. When it is finished, the modifications have been applied to the NE login.

END OF STEPS

□

Delete an NE Login

Purpose Use this procedure to delete an NE login that is being used for an NE.

Before you begin Read the conceptual information in the "NE Logins and Passwords" (2-8) section.

In step 2, you will have to select an NE. For instructions, see "Select/Deselect NEs or Aggregates on the Map Pane" (2-61).

You cannot delete an NE login with a Super-User Authorization Code from an NE.

Task Complete the following steps to delete an NE login from an NE.

1 Select an NE on the Map window.

OR

Select no NE at this point.

2 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

3 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

4 Select **NE Login Administration** from the Security sub-menu.

If you did not choose an NE in Step 1, the Choose an NE window is displayed. Choose an NE from the list by double-clicking on the NE's TID. The chosen NE is highlighted. Click the OK button.

Result:

The Manage NE Login window for the chosen NE is displayed, showing the current list of NE logins.

5 Select the NE login to be deleted from the list of NE logins.

6 Click the Delete button.

Result:

A pop-up window is displayed, asking if you really want to delete the NE login.

7 Select **Yes** to delete the NE login.

END OF STEPS

□

Terminate a User Session

Purpose

Use this procedure to terminate one or more active user login sessions. When you terminate an active user session, the system gracefully exits out of the current session and does not cause any pending or scheduled tasks to be aborted. The user login that was terminated can start a new login session after the login/password is validated.

Before you begin

Determine if the user is currently on the system via the Display Users window.

Task

Complete the following steps to terminate one or more active user login sessions.

1 Access the Map window.

2 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

3 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

4 Select **Terminate User Session** from the Security sub-menu.

Result:

The Terminate EMS User Sessions window is displayed.

5 Select the user login(s) to be terminated from the Users Currently Logged list and, using the arrow push buttons, move the selected user login(s) to the User Sessions to be Terminated list. You can use the arrow push buttons to move user logins back and forth between the two lists, as needed.

6 Click the OK button.

Result:

A pop-up question dialog window is displayed, confirming that you have selected to terminate the user(s) session and asks if you to want to continue with the termination.

7 Choose Yes.

Result:

Active GUI sessions for the user(s) selected are terminated.

END OF STEPS

□

Enable/Disable User Logins

Purpose Use this procedure to enable or disable user logins. Disabling a user login prevents that user from being able to log into the Navis™ Optical EMS. If you disable a user login that is currently on the system, that user's GUI session is automatically terminated. If there is a standing alarm against a user login that has been disabled, re-enabling the user login clears the alarm against it.

Before you begin The `ems` login and other pre-defined logins may not be disabled. To determine if a user is currently on the system, access the List EMS Active Users window through the GUI.

Task Complete the following steps to enable or disable one or more user logins for starting a GUI session.

1 Access the Map window.

2 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

3 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

4 Select **Disable/Enable Users** from the Security sub-menu.

Result:

The Disable/Enable User Sessions window is displayed.

5

TO...	**SELECT...**
disable one or more users	the user(s) in the Enabled Users list and move the user(s) to the Disabled Users list, using the arrow push buttons.
enable one or more users	the user(s) in the Disabled Users list and move the user(s) to the Enabled User list, using the arrow push buttons.**Important!** Use the arrow push buttons to move users back and forth between the two lists, as needed.

6 Click the OK button. If you are disabling one or more users, a pop-up confirmation window is displayed, asking if you really want to prevent the selected user(s) from establishing login sessions. Choose Yes to disable the user(s). If you are enabling one or more users, a pop-up window is displayed asking if you want to enable the selected users. Choose Yes to enable the user(s).

END OF STEPS

□

List EMS Active Users

Purpose This procedure is used to display all users that are currently logged into the Navis™ Optical EMS.

Task Complete the following steps to display all users that are currently logged into Navis™ Optical EMS.

1 Access the Map window.

2 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

3 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

4 Select **List EMS Active Users** from the Security sub-menu.

Result:

The Display Users window is displayed, showing, in table format, a list of users that are currently logged into the system, their user alias, and their login source.

5 Click the Close button to close the window.

END OF STEPS

□

List Active NE Users

Purpose Use this procedure to display all users that are currently logged into the specified NE(s).

Task Complete the following steps to display all users that are currently logged into the specified NE(s).

1 Access the Map window.

2 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

3 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

4 Select **List NE Active Users** from the Security sub-menu.

Result:

The Select NE Active User List window is displayed.

This window is divided into two portions. The left portion of the window lists all of the NEs that are available to obtain a list of active users. The right portion of the window lists that NE(s) that you have selected for the active user listing.

5

TO...	DO THIS...
Show all NEs in your Target Group	Click the Show NEs radio button or do nothing (all NEs are available for selection, by default).

TO...	DO THIS...
Narrow the list of NEs available for selection to a specific NE type	Click the List by Type radio button. Choose the NE type by clicking the down arrow to the right of the List by Type radio button to display a drop-down list, and choose the NE type from the list.

6 Choose one or more NEs from the Network Elements portion of the window and move the NE(s) to the Chosen NEs portion of the window, using the arrow push buttons. You can move NEs back and forth between the two portion of the window, as needed.

7 Once you have made your NE selection(s), click the OK button.

Result:

The ActiveUserLogin Report window is displayed, showing a list of users that are currently logged into the selected NE(s).

If the request for active user logins for the NE has completed, the status in the Status field on the window is ***Completed*** and a message in the status bar on the window indicates that the request has successfully completed for the chosen NE(s). If the request has not completed yet, or failed, the Status field indicates that the request is ***Incomplete*** or ***Failed*** and a message in the status bar indicates that the request is still being processed or has failed.

8 To obtain details about the Status of the request for an NE, double-click on the line for the NE on the Active User Report window.

Result:

The User Login Report Details window is displayed.

This window provides additional information about the Completed, Incomplete, or Failed status of the response by the NE for a list of users currently logged into the NE.

9 To save the output from the window to a file, do the following,

1. Click on **File** on the menu bar on the window and then select **Save As**. A pop-up window is displayed.
2. Select the PC drive where the file folder resides in which to store the file output by clicking the down arrow next to the “Look In” field on the window. Select the drive.
3. Select and open the file folder for the saved output file by double-clicking on the folder in the scrollable list on the pop-up window.
4. Type a name for the output file in the File name field.
5. Click the Save button. The output is saved to the named file.

Important! To view the saved output file, use the Wordpad application.

10 To print a copy of the active users report obtained, choose **File** on the window menu bar and use the following options:

- **Print Setup**- choose this option from the File sub-menu to choose which field from the Active Users Report to print. Click the Landscape or Portrait radio button to print the list in landscape or portrait mode. Use the arrow push buttons to move fields from the total list of fields from the left display column to the “Chosen Fields” display column on the right side of the window. Move fields back and forth between columns as necessary. When you have made your selections, click the OK button. Click the Cancel button to cancel the print setup operation and exit the window.

- **Print Preview** - choose this option from the File sub-menu to preview what the Active Users Report will look like when printed. If alarms are not listed, a message is displayed. After you have finished previewing the output online, choose **File** from the Print Preview window menu bar and then choose **Close** to close the window.
- **Print** - choose this option to print the Active Users Report. When you choose this option, a pop-up Print window is displayed, allowing you to select the printer, number of copies, and other parameters for printing. When you have made your selections on the pop-up Print window, click the OK button and the copy or copies are printed to the selected printer destination. If the Alarm List does not contain any alarms, a message is displayed.

11 To close the ActiveUserLogin Report window, choose **File** from the window menu bar and then choose **Close** to close the window.

END OF STEPS

□

Globally Provision User Login/Password Parameters (Global Security Provisioning Feature)

Purpose Use this procedure to globally administer certain aspects of user login/password procedures enforced by Navis™ Optical EMS, such as the number of login attempts allowed, the login expiration period, the password aging interval, and the password history.

Before you begin Make sure that you are the administrator or a user with a privileged login allowed to provision these login/password parameters.

Task Complete the following steps to globally provision login/password parameters for users logging into the Navis™ Optical EMS.

1 Access the Map window.

2 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

3 Select **Security** from the Administration menu.

Result:

The Security sub-menu is displayed.

4 Select **Global Security Provisioning** from the Security sub-menu.

Result:

The Global Security Provisioning window is displayed.

5 Fill in the following fields, as needed:

- Allow user unsuccessful login attempts before disabling login ID—click the up and down arrows on this spinner field to select the number of consecutive failed login attempts before disallowing a user to log into the system. The default is three tries.
- Delete login IDs after ***x***days of user inactivity—click the up and down arrows on this spinner field to select the number of days that a user login is not in use before it expires (in other words, cannot be used to log into the system). The default is 45 days.
- Prompt users to change passwords every ***x***days—click the up and down arrows on this spinner field to select the number of days that a password can be used before it has to be changed. The default is 30 days.
- Warn users ***x***days prior to their password aging—click the up and down arrows on this spinner field to select the number of days prior to passwords expiring that a warning notice is issued. The default is seven days.
- Remember users' last ***x***previous passwords (and don't allow users to use these previous passwords)—click the up and down arrows on this spinner field to select the number of previous passwords recalled and prohibited from being re-used. The default number is five passwords.
- Restrict Multiple Login Types—Select one value from the displayed list (All, Non-Defined, Pre-Defined, None). If there are multiple active sessions for the login type chosen, then a warning message is issued that having multiple login sessions will terminate all of the multiple active sessions for those users. If you confirm this by clicking on "Yes" when the warning dialog message window is displayed, all of the multiple active sessions are terminated. Then only one session per login for that login type is allowed. If multiple sessions are not active for that login type, then a warning message is not displayed, but the settings are changed in Navis™ Optical EMS. In this case, if a user of a certain login type tries to log in from more than one session, the login attempt is denied. Only one login session is permitted.

- Session inactivity timeout interval—click the up and down arrows on this spinner field to select, in minutes, the session inactivity timeout interval before the user’s GUI session automatically terminates. The default is 30 minutes. Setting the timeout interval to zero disables session timeout; a GUI session does not automatically terminate.
- Enter an advisory message that users will see upon login—enter the text advisory message that is displayed to the user upon successfully logging into the Navis™ Optical EMS.

Important! Click the Get Defaults button to retrieve and display the system defaults for the numeric value fields.

6 Click the Apply button to activate your choices, or click the OK button to activate your choices and close the window.

END OF STEPS

□

Convert to Trusted Mode System

Purpose Use this procedure to convert the Navis™ Optical EMS host operating system to a ***trusted mode*** system.

In addition to the security mechanisms available in the standard UNIX environment, HP-UX offers a utility for converting a host system into a ***trusted*** system that offers a greater security via more stringent password and authentication policies.

Before you begin Conversion to a trusted system should only occur after a successful coldStart installation has been completed. For details about coldStart installation procedures, see the *Navis™ Optical EMS Installation Guide*. In many cases, the ColdStart program needs to be re-run after the conversion. However, the system must be converted back to non-trusted mode before re-running ColdStart.

Before converting to a trusted system, the locally defined NIS server and client have to be removed using the HP SAM tool. Otherwise, the conversion will not proceed. If the conversion still fails after removing the NIS server/client, check the file */etc/rc.confg.d/namesvrs* to make sure that NIS_MASTER_SERVER, NIS_SLAVE_SERVER and NIS_CLIENT are all set to 0.

Task Complete the following steps to convert the Navis™ Optical EMS host operating system to ***trusted mode***.

1 Using the HP SAM tool, highlight **Auditing and Security** and press the Enter key.

2 Highlight **System Security Policies** and press the Enter key.

3 At the confirmation window, select **Yes** to begin the conversion process.

4 At the confirmation window for VxFS Note, select **Yes**.

5 At the Messages window, following the conversion, click the OK button.

6 From the System Security Policies window, do the following:

- Highlight **Password Format Policies** and press the Enter key
- Select User Specifies (only this option)
- Set the Maximum Password Length to 8 and click the OK button
- Select **Password Aging Policies**, select **Disabled**, and click the OK button.
- Select **General User Account Policies** and make the following selections:
- **Lock Inactive Accounts**, set to Disable
- Set **Unsuccessful Login Tries** to 20
- Click the OK button
- Select **Terminal Security Policies**, set **Unsuccessful Login Tries Allowed** to 20, and click the OK button

7 Click the OK button on the main window.

END OF STEPS

□

Turn Off Trusted Mode (Revert Back to Non-Trusted Mode System)

Purpose Use this procedure to revert to a non-Trusted Mode Navis™ Optical EMS host operating system.

Related task For related information, refer to "Convert to Trusted Mode System" (2-58)

Task Complete the following steps to convert the Navis™ Optical EMS host operating system back to a non-Trusted Mode system.

1 Log in as ***root***.

2 Access the HP SAM tool.

3 Highlight **Auditing and Security** and press the Enter key.

4 Highlight **Audited Events** and press the Enter key.

5 Tab to the Main menu.

6 Choose **Actions**.

7 Choose **Unconvert the System**.

Result:

A confirmation window is displayed.

8 At the confirmation window, choose **Yes**

9 Exit the SAM tool.

END OF STEPS

□

Select/Deselect NEs or Aggregates on the Map Pane

Purpose Use this procedure to select and/or to deselect NEs or aggregates on the Map pane.

Task Use this procedure to select ***a single NE or aggregate*** on the Map pane.

1 Position the mouse pointer over the NE or aggregate icon.

2 Click the select mouse button.

END OF STEPS

Task Use this procedure to select ***a group of NEs or aggregates*** on the Map pane.

1 Position the mouse pointer over a portion of the background adjacent to the items to be selected.

2 Click the mouse select button and drag the mouse pointer.

Result:

As you drag the mouse pointer, an outlined box appears over the selected area.

3 Drag the mouse pointer over the NE(s)/aggregate(s) to be selected, enclosing them in the selection box.

Result:

As items in the Map pane are selected, they change color.

4 Release the mouse select button.

Result:

The items are selected.

END OF STEPS

Task Use these steps to deselect ***a single selected item*** in the Map pane.

1 Position the mouse pointer over the item and To deselect a group of items, position the mouse pointer within the boxed region and single-click the mouse select button. Any item in the box that is already selected becomes deselected.

2 Single-click the mouse select button.

Result:

The item is deselected.

END OF STEPS

Task Use these steps to deselect ***a group of selected items*** in the Map pane.

1 Position the mouse pointer within the boxed region.

2 Single-click the mouse select button.

Result:

Any item in the box that is already selected becomes deselected.

END OF STEPS

□

3 System Administration for Standalone Configurations

Overview

Purpose

This chapter describes the procedures for stopping, restarting, and rebooting a standalone, (non-redundant) Navis™ Optical EMS application.

Contents

□

Bring Down the Navis™ Optical EMS Application

Purpose

The Navis™ Optical EMS application runs continuously on the standalone (non-redundant) server under normal operating conditions, gathering and routing network information. This procedure explains how to stop the execution of the application on a standalone server.

Before you begin

The application is typically stopped ***only*** under the following conditions:

- The server must be rebooted.
- The Navis™ Optical EMS database needs to be restored.
- A power outage affects the server.
- A Navis™ Optical EMS problem needs to be corrected.

Task

Complete the following steps to bring down the Navis™ Optical EMS application.

1 Log in to the Navis™ Optical EMS server using the `ems` login.

2 At the system prompt type `dn –x` and press the Enter key.

3 After the application has been brought down, verify that it is in shutdown mode by typing `appstat` and then pressing the Enter key.

Result:

A message indicating that the application has been shut down is issued.

END OF STEPS

□

Bring Up the Navis™ Optical EMS Application

Purpose This procedure is used to bring up the Navis™ Optical EMS application on a standalone, non-redundant server.

Before you begin In this procedure, the system asks whether you want to delete trace files. Trace files should be deleted (answer `y`) unless they are needed to diagnose a system problem.

Task Complete the following steps to bring up the Navis™ Optical EMS application.

1 Log on to the Navis™ Optical EMS server using the `ems` login.

2 At the system prompt type `up` and press the Enter key.

Result:

The system displays a prompt asking whether to delete the trace files.

3 Answer the system prompt regarding trace files accordingly with a `y` or an `n`.

4 Confirm that the application is running and that processes are not respawning by typing `appstat` and then press the Enter key.

Result:

A list of all processes with corresponding information is displayed, followed by the status of the current Run Level.

END OF STEPS

□

Reboot the Navis™ Optical EMS Application

Purpose This procedure is used to reboot the Navis™ Optical EMS application with the **shutdown** command, which gracefully shuts down the application and the Informix database and reboots the system.

Before you begin Before rebooting the application using the **shutdown** command, the system console ***must*** be powered on.

The format of the **shutdown** command is: **shutdown <-r> <-y> <time>**; where: **-r** is reboot; **-y** is yes; and **0** is now.

Task Complete the following steps to reboot the Navis™ Optical EMSapplication.

1 Log in as `root` to the HP server that is running the Navis™ Optical EMSapplication.

Result:

The # system prompt is displayed.

2 At the system prompt, type `/etc/shutdown -r -y 0` and press the Enter key.

END OF STEPS

□

4 Database Maintenance

Overview

Purpose This chapter provides basic procedures for backing up and restoring the Navis™ Optical EMS database and exporting the database.

Before you begin The procedures described in this chapter assume that you are working with a Navis™ Optical EMS database from the same release. If you are converting a Navis™ Optical EMS database from a different release, call 1-800-225-4672 for technical assistance.

Contents

□

Change the Default Tape Size in the onconfig File

Purpose

This procedure is used to change the default tape size in the *onconfig* file from 1GB, which was the standard ***older*** default tape size, to the maximum amount of data that can be now be stored, which is 2GB or 4GB.

The default tape size should be changed in the *onconfig* file to avoid using more than one tape to backup the Navis™ Optical EMS application database.

Before you begin

Make sure that you have the proper DDS drive in the HP server and that you are using the proper DDS tape.

Beware that the amounts of data that can be stored are as follows:

- ***102400 KB***, which is 1 GB—the default.
- ***204800 KB***, which is 2GB—a more current, maximum value.
- ***4096000 KB***, which is 4GB—a more current, maximum value.

Task

Complete the following steps to change the default tape size from 1GB in the *onconfig* file.

1. Log in as `ems`.

2. Enter the following command line: `su –informix`

3. Enter the following command line: `cd /tolls/informix/etc`

4. Use the `vi` editor to access the *onconfig* file: `vi onconfig`

5. Search for the value of `TAPESIZE` and change the value of `102400` to `2048000` for a 2GB tape or `4096000` for a 4GB tape.

6. Save the changes made to the file and exit from the `vi` editor.

7 Use the following command line to take Informix off line: `onmode –ky`

8 Use the following command line to put Informix on line: `oninit`

9 Bring up the application.

Result:

The Navis™ Optical EMS application database is now on one tape.

END OF STEPS

□

Back Up the Navis™ Optical EMS Application Database

Purpose

Maintaining tape backups of the database is critical to the overall reliability of the Navis™ Optical EMS application. If a hardware failure or other mishap occurs, service disruptions resulting from loss of data can be minimized when a recently backed-up version of the database is available.

Before you begin

Consider the following as you prepare to backup the database:

- You must be able to physically access the HP server that is running the Navis™ Optical EMS application to insert and remove backup tapes.
- The database should be backed up at least once a week—more frequent backups should be made when user activity is high.
- A backup should be also verified and saved permanently off-site every six months to safeguard against problems resulting from a faulty tape and/or tape drive.
- A backup of the application database requires one or more tapes depending upon the database size.
- Backup tapes should be labeled with the date and contents of the tape as instructed by the Informix backup and restore processes.

Task

Complete the following steps to back up the application.

1 Insert a tape into the tape drive of the HP server running the Navis™ Optical EMS application.

2 To archive the database, log in as the Informix user. You can do this while logged in using your normal login by typing `su - informix` and pressing the Enter key. (su - informix needs a space before and after dash).

Important! The Navis™ Optical EMS application does not have to be brought down to perform a backup.

3 At the system prompt, type `ontape -s -L 0` and press the Enter key.

Important! A backup can take anywhere from 30 minutes to several hours, depending on the amount of data.

Result:

The following prompt is displayed:

```
Please mount tape 1 on /dev/rmt/0m and press the
Return/Enter key to continue.

10 percent done.

100 percent done.
```

4 When the backup is complete, messages similar to the following appear:

```
Please label this tape as number 1 in the arc tape
sequence.

This tape contains the following logical logs:

126

Program over.
```

END OF STEPS

□

Restore the Navis™ Optical EMS Application Database

Purpose This procedure is used to restore the Navis™ Optical EMS application database.

Before you begin The Navis™ Optical EMS application ***must*** be brought down and Informix must be taken off-line to execute the restore procedure, and you ***must*** have the same database configuration.

Task Use these steps to restore the Navis™ Optical EMS application database.

1 Log into the HP server running the Navis™ Optical EMS application as ***ems***.

2 Bring the application down by typing `dn –x` and pressing the Enter key at the system prompt.

3 Log into Informix by entering `su - informix` at the system prompt. Press the Enter key.

4 Verify that you have a correct *onconfig* file and *sqlhosts* file in */tools/informix/etc* directory and a *.profile* in the */tools/informix* directory.

5 Type `onmode -ky` and press the Enter key to bring the Informix server off line.

6 To start the restore process, type `ontape -r` at the system prompt and press the Enter key.

Result:

Prompts are displayed similar to:

```
Continue Restore (y/n): y

Do you want to back up the logs? (y/n): n

Restore a level 1 archive? (y/n): n
```

```
Do you want to restore log tapes? n
/tools/informix/bin/onmode -sy
Program over.
```

7 Type `onmode -m` and press the Enter key to put Informix in on-line mode

8 To confirm Informix is on-line, type `onstat -` and press the Enter key.

Result:

The output is similar to the following:

```
INFORMIX-OnLine Version 7.31 uc2xc--On-Line--Up
00:23:56 --- 116936 Kbytes
```

9 Log out of Informix and log back into ***ems*** by typing `exit` and pressing the Enter key.

10 Start the Navis™ Optical EMS application by typing `up` and press the Enter key at the system prompt.

END OF STEPS

□

Back Up Key Data from the Navis™ Optical EMS Application

Purpose

This procedure is used to back up key Navis™ Optical EMS application data and database data, including the NE directory information that the Directory Services Agent (DSA) maintains. You can back up one database or set of application data. You can back up the data to a single tape or multiple tapes.

Before you begin

You will be using the **ems_backup** command. The syntax of the command is:

```
ems_backup [-d EMS|CF|PM|NCI|] [-one] [-app]
```

where:

`-d` specifies to back up one database at a time:

`EMS` specifies the Informix database.

`CF` specifies Configuration data.

`PM` specifies Performance Monitoring data.

`NCI` specifies CORBA interface data.

`-one` specifies to back up all data onto one tape. The default is multiple tapes. If the `-one` option is used, insert one blank tape in the tape drive and execute the command **ems_backup -one**.

`-app` specifies to back up only the application data and DSA data.

Important! If options are not specified, the system prompts you for all database types. But, before any prompt is given, DSA data is written to tape. Once the first prompt is received, the tape must be changed to prevent data from being over-written.

Task

Complete the following steps to backup the required application data or database data.

1 Insert a tape into the tape drive of the HP server running the Navis™ Optical EMSapplication.

2 Log into the server using the `ems` login.

Result:

The UNIX system prompt appears.

3 Enter the command `ems_backup` using the command syntax provided in ***Before you begin***.

Result:

The system flat files for the selected backup data are immediately written to the tape.

4 If multiple tapes are being used for the backup, insert the next tape into the tape drive.

END OF STEPS

□

Restore Key Data from the Navis™ Optical EMS Application Database

Purpose

This procedure is used to restore key data in the Navis™ Optical EMS application database, including the NE directory information maintained by the Directory Services Agent (DSA). You can restore one database or a set of application data at a time. You can restore the data from a single tape or multiple tapes.

Before you begin

You will use the **ems_recover** command. The command syntax is:

```
ems_recover [-d EMS|CF|PM|NCI|][-app]
```

where:

`-d` specifies to restore one database from tape.

`EMS` specifies the Informix database.

`CF` specifies Configuration data.

`PM` specifies Performance Monitoring data.

`NCI` specifies CORBA interface data.

`-app` specifies to restore only the application data and DSA data from tape.

Task

Complete the following steps to restore the required application data or database data.

1 Log into the HP server running the Navis™ Optical EMS application using the `ems` login.

Result:

The UNIX system prompt appears.

2 Enter the command `ems_recover`, using the syntax provided in the ***Before you begin*** section.

END OF STEPS

□

Export the Navis™ Optical EMS Application Database to a Directory

Purpose

This procedure is used to export the Navis™ Optical EMS application database to a directory. A copy of the database can also be exported to an ASCII text format, which allows you to transfer the database to another Informix environment that is configured differently.

Before you begin

The application ***must*** be shut down before doing a database export. Back up the */ems/dsa* directory to ensure system consistency after a restart.

Task

The following procedure is used to perform a database export to a directory.

1 Log in as `ems`.

2 Bring the application down.

3 At the UNIX prompt, use the following commands to back up the application database to a directory. Execute each command individually:

`dbexport $EMS_DBNAME -c -ss -o <directory>`

`echo $NUMOFCFDBS`

`dbexport ${CF_DBNAME}n -c -ss -o <directory>` n is a single digit number from 1 to $NUMOFCFDBS. Repeat the command with a different number (n) if n>1

`dbexport $PM_DBNAME -c -ss -o <directory>` (only if PM is collected)

`dbexport $NCI_DBNAME -c -ss -o <directory>` (only for CORBA interface)

Result:

After each **dbexport** command, the message `dbexport complete` indicates the procedure has been successfully completed.

END OF STEPS

□

Export the Navis™ Optical EMS Application Database to Tape

Purpose

This procedure is used to export the Navis™ Optical EMS application database to tape.

Before you begin

The application ***must*** be shut down before doing a database export. Back up the */ems/dsa* directory to ensure system consistency after a restart.

This procedure requires multiple tapes; so, have them available.

Procedure

Complete the following steps to export the application database to tape.

1 Log in as `ems`.

2 Bring the application down.

3 At the UNIX prompt, use the following commands to back up the application database to tape.

Note: Mount a new tape before executing each command. Each command may require more than one tape. Swap tapes by following system prompts.

```
dbexport $EMS_DBNAME -c -ss -t /dev/rmt/0m -b 512 -s 2000000
```

```
echo $NUMOFCFDBS
```

```
dbexport ${CF_DBNAME}n -c -ss -t/dev/rmt/0m -b 512 -s 2000000
```

Note: n is a single digit number from 1 to $NUMOFCFDBS. Repeat the command with a different number (n) if n>1.

`dbexport $PM_DBNAME -c -ss -t /dev/rmt/0m -b 512 -s 2000000` (only if PM is collected)

`dbexport $NCI_DBNAME -c -ss -t /dev/rmt/0m -b 512 -s 2000000` (only for CORBA interface)

Result:

After each **dbexport**command, the message `dbexport complete` indicates the procedure has been successfully completed.

END OF STEPS

□

Import the Navis™ Optical EMS Application Database from a Directory

Purpose

This procedure is used to import the Navis™ Optical EMS application database from a directory. A copy of the database can also be ***imported*** from a database exported by `dbexport` .

Before you begin

The Navis™ Optical EMS application ***must*** be shut down before doing a database import. You must restore */ems/dsa* directory to ensure system consistency after restart.

Task

Complete these steps to import the application database from a directory.

1 Log in as `ems`.

2 If a Navis™ Optical EMS database exists, drop it by running the following command at the UNIX prompt (be careful using this command):

```
drdb
```

3 Use the following commands at the UNIX prompt:

```
dbimport $EMS_DBNAME -d snc_dbs -c -i <directory><Enter>
```

```
echo $NUMOFCFDBS
```

```
dbimport ${CF_DBNAME}n -d snc_dbs -c -i <directory><Enter>
```

Note: n is a single digit number from 1 to $NUMOFCFDBS. Repeat the command with a different number (n) if n>1.

```
dbimport $PM_DBNAME -d pm1_dbs -c -i <directory><Enter>
```
(only if PM is collected)

```
dbimport $NCI_DBNAME -d nb_dbs -c -i <directory><Enter>
```
(only for CORBA interface)

Result:

After each **dbimport** command, the message `dbimport complete` indicates the procedure has been successfully completed.

4 Use the following commands at the UNIX prompt to activate logging:

```
db_logging -U $EMS_DBNAME
```

```
echo $NUMOFCFDBS
```

`db_logging -U ${CF_DBNAME}n` n is a single digit number from 1 to $NUMOFCFDBS. Repeat the command with a different number (n) if n>1.

```
db_logging -U $PM_DBNAME
```

```
db_logging -U $NCI_DBNAME
```

END OF STEPS

□

Import the Navis™ Optical EMS Application Database from Tape

Purpose This procedure is used to import the Navis™ Optical EMS application database from tape.

Task Complete the following steps to import the application database from tape.

1 Log in as `ems`.

2 If an application database exists, drop it by running the following command at the UNIX prompt (be careful using this command):

```
drdb
```

3 Use the following commands at the UNIX prompt:

```
dbimport $EMS_DBNAME -d snc_dbs -c -t /dev/rmt/0m -b 512
-s 2000000
```

```
echo $NUMOFCFDBS
```

```
dbimport -U ${CF_DBNAME}n-d snc_dbs —c —ss —t/dev/rmt/0m
—b 512 —s 2000000
```

Note: n is a single digit number from 1 to $NUMOFCFDBS. Repeat the command with a different number (n) if n>1.

`dbimport $PM_DBNAME -d pm1_dbs -c -t /dev/rmt/0m -b 512 -s 2000000` (only if PM is collected)

`dbimport $NCI_DBNAME -d nb_dbs -c -t /dev/rmt/0m -b 512 -s 2000000` (only for CORBA interface)

Result:

After each **dbimport** command, the message `dbimport complete` indicates the procedure has been successfully completed.

4 Use the following commands at the UNIX prompt to activate logging:

```
db_logging -U $EMS_DBNAME
```

```
echo $NUMOFCFDBS
```

`dblogging -U ${CF_DBNAME}n` n is a single digit number from 1 to $NUMOFCFDBS. Repeat the command with a different number (n) if n>1.

```
db_logging -U $PM_DBNAME
```

```
db_logging -U $NCI_DBNAME
```

END OF STEPS

□

5 Management Communication

Overview

Purpose This chapter explains how to set up the interfaces to communicate with the NEs for all supported communication protocols.

Contents

□

Configure OSI Communication on the HP Server

Purpose

This procedure is used to configure OSI on the HP server that is used as the Navis™ Optical EMS host.

The Navis™ Optical EMS IAO-LAN interface provides an OSI standard, high-speed communications path to NEs. It enables the reduction of performance bottlenecks by providing faster communications between the EMS and NEs. The OSI LAN interface provides up to three high bandwidth communication paths or OSI associations to NEs. This communication model is based on the standard 7-layer OSI stack reference model.

Before you begin

Before you run **installEms**, the LAN card should be configured. The items you will need follow:

- The OSI LAN requires a separate LAN card—the configuration requires one LAN card for the Navis™ Optical EMS local LAN and another card for the OSI-to-NE communication.
- Each LAN card should be connected to a different hub because the hubs can sometimes cause communication problems.
- LAN redundancy requires two LAN cards for OSI. For additional redundancy, a separate hub should be created for each LAN card. (Remember—the workstation LAN card cannot be used for redundancy; another LAN card must be purchased for OSI support.)
- LAN Cards 0 and 1 are located on the back of the HP server. On the server, LAN cards are counted from top left to bottom right.
- When using external LAN cards, power down the server and move the LAN card jumpers from INT to EXT. The front two jumpers should be ***on***.
- Both LAN cards, the IP LAN card and the Southbound LAN card, should be on a different SUBNET.

Task

Complete the following steps to configure OSI on the HP server.

1 Bring down the application by typing `dn`.

2 su to root.

3 Use lanscan to get the number or MAC address of the LAN card. (This is also done automatically.)

4 Run `installEms`.

5 Select option `#4) Configure EMS` to make the provisioned parameters effective.

Result:

You are prompted to select the OSI configuration options.

END OF STEPS

□

Configure OSI and TCP/IP Communication on Separate LAN Cards

Purpose

This procedure is used to configure OSI and TCP/IP on separate LAN cards.

Before you begin

The LAN cards should be configured before running install.

To configure OSI and OSI over TCP/IP communication on different network interfaces, a total of at least three network cards are needed: one for general network purposes (remote shell/support), one for OSI, and one for OSI over TCP/IP communication.

Example: In the three LAN cards shown, lan0 is used for OSI; lan1 is used for OSI over TCP/IP; and lan2 is used for general network purposes.

```
# lanscan

Hardware Station Crd Hdw Net-Interface NM MAC HP-DLPI DLPI

Path Address In# State Name PPA ID Type Support Mjr#

10/4/4.1 0x0800095A7953 0 UP lan0 snap0 1 ETHER Yes 119

10/4/8 0x001083348188 1 UP lan1 snap1 2 ETHER Yes 119

10/12/6 0x001083278A69 2 UP lan2 snap2 3 ETHER Yes 119
```

Task

Complete the following steps to configure OSI and TCP over OSI communication on different network interfaces.

1 Configure the LAN cards (lan0 for OSI, lan1 for OSI over TCP/IP, lan2 for general network purposes):

```
# ifconfig lan0

lan0: flags=843<UP,BROADCAST,RUNNING,MULTICAST> inet
172.100.100.50 netmask ffff0000 broadcast 172.30.255.255

# ifconfig lan1

lan1: flags=843<UP,BROADCAST,RUNNING,MULTICAST> inet
192.192.0.100 netmask ffff0000 broadcast 192.192.255.255

# ifconfig lan2
```

```
lan2: flags=843<UP,BROADCAST,RUNNING,MULTICAST> inet
135.10.100.100 netmask ffff0000 broadcast 135.17.255.255
```

2 Run installEms.

3 Select `option #4) Configure EMS` to make the provisioned parameters effective.

4 The following screen output is displayed. (User input is shown.)

Do you wish to continue with this installation (y/n)?

y

Do you wish to backup the EMS application database (y/n/q)?

n

1. CD-ROM

2. Digital Audio Tape (DAT)

Please enter the software media type [1/2/q]?

Are you ready to proceed? (y) to proceed, <CR> to skip, or (q) to quit:

y

Hit <CR> to continue ....

<CR>

Are you ready to proceed? (y) to proceed, <CR> to skip, or (q) to quit:

The EMS new host Informix Database configuration is about to begin.

The Informix Database configuration will use socket instead of share memory. Please adjust your Name Service Switch accordingly.

Do you want to continue this process (y/n/q):

n

Press [ENTER] to continue.

5 The system responds with:

```
The following LAN interface(s) have been detected:
lan 0 10/4/4 lan0 CLAIMED INTERFACE HP J2146A - 802.3 LAN
lan 1 10/4/8 lan1 CLAIMED INTERFACE HP J2146A - 802.3 LAN
lan 2 10/12/6 lan2 CLAIMED INTERFACE Built-in LAN
Press [Enter] to continue
1. Network Service Attachment Point (NSAP) forms (Fixed/Flexible)?:
Fixed
2. Activate SONET Directory Services (y/n)?: y
3. NE PROTOCOL INFORMATION
The current configuration is displayed:
CMISE: (y/n) Y
OSI TL1: (y/n) Y
X.25 TL1: (y/n) Y
Please enter the item number [1-3] to make change.
Enter "s" to save the above input and continue.
Enter "q" to quit.
s
```

6 The current OSI Configuration is summarized as following:

```
1. Primary OSI LAN interface number= 1
2. Organization Identifier= 000000
3. Routing Domain= 0000
4. OSI Area= 0000
5 OSI Lan Redundancy is not configured.
6. IP address for OSI over TCP/IP= 192192000100
```

We are using lan0 for OSI communications, but we entered the IP address for lan1 for TCP/IP over OSI communications. Changing these options is very easy, as explained below by following the prompts. The rest of the steps are self-explanatory.

```
Enter the item number [1-6] to change the current value.
Enter "s" to save the above input and continue.
```

```
What would you like to do [1-6, or s] [q to quit]: s
```

7 Continue the install.

END OF STEPS

□

Configure the Transport Bridge and the Registration Manager on the WaveStar™ OLS 1.6T

Purpose This procedure is used to configure both the transport bridge and the registration manager for the WaveStar™ OLS 1.6T.

Before you begin Realize that one Registration Manager (RM) is needed per OSI area.

DSA must be configured before the EMS allows any NEs to register in the database.

Task From the NE, the following commands are needed to provision the WaveStar™ OLS 1.6T to be both a Transport Bridge and a Registration Manager.

1 If the NE is going to be a transport bridge, input the ENT-SYS (enter system) command to assign an IP address to the NE's OS port. The command syntax follows:

```
ENT-SYS:TID::CTAG:::[Spec_block];
```

Example:

```
ENT-SYS:WSOLS400G-----12345678-::XXX:::
IP_ADDRESS=123.456.789.012,DFLTRTR_IPADDRESS=123.456.789.01
LOCAL_SUBNETMASK=255.255.255.0;
```

1. The IP_ADDRESS is the IP address that the network administrator has given to the NE.
2. The DFLTRTR_IP ADDRESS is the IP address of the default gateway.
3. If LOCAL_SUBNETMASK is entered, the NE resets.

2 For each OSI area, enter the ENT-RMA (enter-registration manager) command to enter the registration manager. The command syntax follows:

```
ENT-RMA:TID:SYSTEM:CTAG:::[Spec_block];
```

Example:

```
ENT-RMA:WSOLS400G-----12345678-:

SYSTEM:XXX1:::
```

```
RM_ACTIVE=ENABLE,DSA_PSEL=0123,DSA_SSEL=012345

DSA_TSEL=012345,

PRI_DSA_NSAP=1339840F80000000000000000000xxxxxxxxxxxx,

PREFIX_COUNTRY=US,PREFIX_ORG=LUCENT,PREFIX_
SUBORG1=EMS1;
```

1. If a transport bridge is not required (for pure OSI communication only), specify the PRI_DSA_NSAP (primary DSA NSAP), which is the NSAP of the Navis™ Optical EMS southbound LAN card prefixed with a 13; the string totals 40 characters.
2. For the DSA_PSEL, DSA_SSEL, and DSA_TSEL—which are the presentation, session and transport layers— the recommended values are shown as 0123, 012345, and 012345, respectively.

3 Use the ENT-TSB (enter-transport bridge) command to enter the transport bridge. The command syntax follows:

```
ENT-TSB:TID:SYSTEM:CTAG:::[spec_block];.

ENT-TSB:WSOLS400G-----12345678-:SYSTEM:XXX:::
PRI_TSB_NSAP=1339840f80000000000000000000xxxxxxxxxxxx,
PRI_DSA_IP_ADDRESS=123.456.789.012;
```

1. The PRI_TSB_NSAP is the NSAP of the transport bridge NE. Obtain the Ethernet address of the NE using the WaveStar® CIT interactive mode RTRV-SYS command.
2. The DSA IP Address is the IP address of the Navis™ Optical EMS southbound LAN.

4 All network NEs should now register themselves with the Navis™ Optical EMS database.

END OF STEPS

□

Set Up OSI Communication on the WaveStar® BWM

Purpose Use this procedure to set up OSI communication for a WaveStar® BWM using the WaveStar® BWM CIT.

For OSI communication, the WaveStar® BWM uses the J175 or J177 DB9 connector for OSI communication, which can be found on the back of the control shelf.

WARNING

Navis™ Optical EMS and the CIT must be plugged into separate ports in the back panel of the main controller. It is recommended that the J175 and J177 DB9 connectors found along the right-hand side of the system controller bay be used. If the J175 or J177 DB9 connectors are already being used for the CIT or a network element, the J176 or J180 connectors can be used for connecting the WaveStar® BWM to the Navis™ Optical EMS. Do not use the front connector or there will be a problem with connectivity.

Task Complete the following steps to set up OSI on the WaveStar® BWM.

1 To retrieve the current configuration:

RTRV-ULSDCCL3:tid:aid:ctag; TL1 Syntax

2 To enter or change the configuration:

ENT-ULSDCCL3:tid:aid:ctag:::spec_block; TL1 Syntax

```
ENT-ULSDCC-L3:BWM tid:SC-1-#-# -dcc1 -cp:ctag
:::L3rd=0000,l3 Area=0000, l3lrds=Enable;
```

END OF STEPS

□

Set Up TCP/IP Communication on the WaveStar® BWM

Purpose This procedure is used to configure the WaveStar® BWMfor TCP/IP communication using the WaveStar® BWM CIT.

For OSI communication, the WaveStar® BWM uses a J175 or J177 DB9 connector, which can be found on the back of the control shelf.

WARNING

The Navis™ Optical EMS and the CIT must be plugged into separate ports in the back panel of the main controller. Use the J175 and J177 DB9 connectors, which are found along the right side of the system controller bay. If the J175 or J177 DB9 connectors are already being used for the CIT or a NE, the J176 or J180 connectors can be used for connecting the WaveStar® BWM to the Navis™ Optical EMS application. Do not use the front connector or there will be a problem with connectivity.

Task Complete the following steps to configure a WaveStar® BWM for TCP/IP communication.

1 Log in to WaveStar® BWM CIT.

2 Enter the IP address in the WaveStar® BWM using the following command:

```
ENT-IP-MAP:TID:AID:CTAG::::SPEC_BLOCK
```

An example of this command is:

```
ENT-IP-MAP-BWMNODENAME:SC-1-#-#-DCC1-CP:RSF:::ACID=TL1MEMORYADMINISTRA
```

For the ACID, the choices are:

- TL1MAINTENANCE
- TL1MEMORYADMINISTRATION
- TL1TEST
- TL1OTHERQ
- TL1PEERCOMM

END OF STEPS

Set Up OSI Communication on the WaveStar™ OLS 1.6T

Purpose The procedure is used to set up OSI on the WaveStar™ OLS 1.6T.

Before you begin The WaveStar™ OLS 1.6T uses the J32OS DB9 connector, which is located in the system bay interconnect panel.

Task Complete the following steps to set up OSI for a WaveStar™ OLS 1.6T.

1 Use the RTRV-OSI command to retrieve the current OSI configuration. The command syntax is RTRV-OSI:TID::ctag;

Example:

```
RTRV-OSI:OLS-400G::rsf

IP 789012

<

OLS-400G 99-10-26 16:42:11

M 789012 COMPLD

“localaddress=39000080,isislvl=Level-2,drp=64”
```

2 Use the ENT-OSI command to enter or change the OSI configuration. The command syntax is ENT-OSI:TID::CTAG:{GEN_BLOCK}{:{:{SPEC_BLOCK}}}

Example:

```
ent-osi:tid::ctag:::localaddress=1339840f800000000000dddd9999

,isislvl=level-2,drp=64;

IP 123456

<

400G 99-10-26 16:42:11

M 123456 COMPLD
```

END OF STEPS

□

Set Up TCP/IP Communication the LambdaRouter™ AOS

Purpose This procedure is used to set up the LambdaRouter™ AOS, which includes obtaining and assigning an IP address for the LambdaRouter™ AOS and configuring it in the application database

Before you begin You will have to log in to the LambdaRouter™ AOS CIT. The default login is ***LUC01***; the default password is ***OXC+1***.

This procedure requires a subnetwork for the LambdaRouter™ AOS. If a subnetwork has not yet been created, you can create the subnetwork in this procedure.

Task Complete the following steps to obtain and assign an IP address for the LambdaRouter™ AOS and to configure it in the application database.

1 Log into the LambdaRouter™ AOS CIT using the CIT default login and password.

2 Select **Administration** from the main menu bar.

Result:

A sub-menu is displayed.

3 Select the appropriate TID from the TID pulldown menu.

Result:

A sub-menu is displayed for selection of the IP address.

4 Select the IP address of the LambdaRouter™ AOS.

Result:

A separate window is displayed to select the system controller (DCC-1–1).

5 Select the system controller.

Result:

A separate window is displayed to input the IP address.

6 Input the IP address.

7 Click the OK button.

8 Log into the Navis™ Optical EMS application.

9 A subnetwork for the LambdaRouter™ AOS needs to be created before it can be added to the Navis™ Optical EMS database, if there is no existing subnetwork with which it can be associated.

IF...	THEN...
A subnetwork needs to be created first before adding the *LambdaRouter*™AOS NE	Choose **Administration** from the main menu bar on the Map window. The Administration sub-menu is displayed. Choose **Network** from the Administration sub-menu. The Network sub-menu is displayed. Choose **Subnetworks** from the Network sub-menu. The Manage Subnetworks window is displayed. Click the Add button. The Add a Subnetwork window is displayed. Enter a Subnetwork Name. Optionally, you can also enter a Subnetwork Alias. Click the OK button to add the subnetwork and close the Add a Subnetwork window.
A subnetwork already exists with which the LambdaRouter™ AOS can be associated	Skip to Step 10

10 Select **Administration** from the main menu bar on the Map window.

Result:

The Administration menu is displayed.

11 Select **Network** from the Administration menu.

Result:

A sub-menu is displayed.

12 Select **Network Elements** from the sub-menu.

Result:

The Manage NEs window is displayed, showing the current list of NEs in your Target Group.

13 Click on the Add button.

Result:

The Add an NE - General Information panel is displayed.

The Add an NE window for TCP/IP NEs is divided into three panels:

- General NE Information
- NE Communications Details (GNE or TCP/IP)
- NE Security

There are fields on each panel that are required to add a GNE. To access a panel, click the mouse select button on the panel's labeled tab.

The General Information panel is displayed initially.

14 Enter the NE's Target Identifier (TID). A TID can be 1 to 20 alphanumeric characters. Hyphens, slashes ("/"), and periods are allowed. This field is required.

15 Enter the NE Alias. An alias can be 1 to 40 alphanumeric characters. Uppercase and lowercase letters are allowed. Spaces are allowed. This field is optional.

16 Select the NE Type. To do this, click the down arrow to the right of the field to display a drop-down list of choices and select the NE type. This field is required.

17 Select the NE time zone by clicking the appropriate radio button. If ***Other*** is selected, enter the time difference, in minutes, between the NE time and Greenwich Mean Time (GMT). Specify the time difference, "+" (plus) or "-" (minus), up to five characters. Valid values are -11.0 to 13.00 (the plus "+" is implied). This field is required. If selection is not made, the time zone defaults to ***Same as Host***.

18 In the Communicate Via field of the General Information panel:

IF ...	CLICK...
The NE is communicating with the Navis™ Optical EMS server via a GNE	the GNE radio button. Go to Step 19.
The NE is communicating directly with the Navis™ Optical EMS server via TCP/IP	the TCP/IP radio button. Go to Step 20 .

19 If you selected the Communicate Via GNE option in Step 18, click on the NE Communications Detail (GNE) panel. Select a GNE from the list on the panel.

Skip to Step 26.

20 If you selected the Communicate Via TCP/IP option in step Step 18, click on the NE Communications Details (TCP/IP) tab. The NE Communications Details (TCP/IP) panel is displayed. This panel is used to enter information about the interface between this GNE, the Navis™ Optical EMS server and the other NEs in the subnetwork.

Important! You must enter a valid IP address for the NE. Navis™ Optical EMS does not check the validity of the IP address entry.

21 The Communication Type defaults to TL1 Only. The other options are currently not available.

22 Click on the down arrow to the right of the Choose a Subnetwork field to display a list of subnetworks, and select a compatible subnetwork. This field is required.

Important! More than one GNE can be associated with a subnetwork name/alias. This enables the load to be shared among multiple GNEs. However, it is important that all of the GNEs associated with a subnetwork name/alias truly are in the same physical subnetwork. Incorrect associations of GNEs to subnetworks may result in Navis™ Optical EMS being unable to establish a connection to some remote NEs in the subnetwork.

23 Enter the NE’s IP address. The IP address field is divided into four 3-character fields separated by periods.

As an option, the LambdaRouter™ AOS allows you to enter a second IP address.

If two IP addresses are entered, the application uses the first IP address to make a connection with the NE. If the first IP address fails for some reason, the application attempts to make a new connection with the NE using the second IP address.

24 For NEs discovered under the GNE being added (Discovered Remotes), choose one of the following options (by clicking on that option’s radio button):

- This GNE—the NE login and password entered for this GNE in the NE Security panel will be used to log into the NEs.
- Navis™ Optical EMS Default for Remote NEs—the system-wide Navis™ Optical EMS default NE login and password for the NE type of the Remote Terminal (RT) being discovered will be used to log into the NEs.
- Navis™ Optical EMS Default for GNE Type—the system-wide Navis™ Optical EMS default NE login and password for the NE type of the GNE being added will be used to log into the NEs.

25 Choose the number of associations for the NE type. This field is required.

Go to step Step 26.

26 Click on the NE Security tab.

Result:

The NE Security panel is displayed.

27 Enter the primary NE login for the NE being added. The login can be 1 to 10 characters.

28 Enter the primary NE password for the NE login. An NE password must be 6 to 10 alphanumeric characters, with at least two non-alphabetic characters, of which one character must be one of the following special characters (# % +). The password must begin with a letter.

29 Re-enter the primary NE password, in the Re-enter Password field, for checking.

30 Enter the backup login for the NE. The backup login can be 1 to 10 characters.

31 Enter the backup password for the NE. An NE password must be 6 to 10 alphanumeric characters, with at least two non-alphabetic characters, of which one character must be one of the following special characters (# % +). The password must begin with a letter.

32 Click the Apply button to activate your choices, or click the OK button to activate your choices and close the NE Security panel of the Add/Modify NE window.

33

IF...	**THEN...**
You are adding a GNE and the system prompts whether DNO should be run at this time to update the Navis™ Optical EMS database with complete information about the newly added NE.	Choose **Yes** to run DNO or **No** to not perform DNO at this time.**Important!** If you are adding more GNEs to the same subnetwork, choose **No** to not perform DNO at this time. A DNO should not be performed until all GNEs in the same subnetwork have been added so new RNEs discovered automatically by Navis™ Optical EMS via a newly added GNE can be reassigned to another GNE in the same subnetwork, if necessary.
You are not adding a GNE	No DNO prompt is displayed. **Result:** A message in the status bar is displayed, indicating that the NE is being added to Navis™ Optical EMS.

END OF STEPS

□

Set Up OSI Communication on the Metropolis™ EON

Purpose This procedure is used to enable the LAN connection for a Metropolis™ EON using the Metropolis™ EON CIT.

Before you begin Verify that the Metropolis™ EON is connected to the J13 port on the front of the system.

You will be required to log in to the CIT. The default login is ***LT01***; the default password is ***FT-2000***.

Task Complete the following steps enable the LAN connection for an Metropolis™ EON using the CIT.

1 Log into the Metropolis™ EON CIT using the CIT default login and password.

2 Enter the following commands:

```
ACT-USER:TID:LT01:RSF::FT-2000;
```

```
ENT-OSI:TID:LEVEL-1,NODEISISLVL=LEVEL-2,DRP=64,TRANSFERMODE=UITS
```

3 Using the Centerlink CIT, choose **Security->Retrieve->Channel Identifier->Security** to set up the LAN connection on the network element.

Result:

A window is displayed. Check the status of the Port Status field to determine if the LAN connection is enabled. If it is not enabled, enable it.

4 Using the Centerlink CIT, choose **Security->Retrieve->OSI** to check the OSI communication.

5 Use the `RTRV-OSI` command to check OSI communication:

```
RTRV-OSI:TID::CTAG;
```

Result:

Output from the TL1 command issued should be similar to the following:

`Local= 39840f8000000000000000000`***<Org, Routing Domain, Area Addresses>***

`open_sid= 08006a0643db` ***<OLS 40G/80G MAC address>***

`>`

`nodeisislvl= 2` ***<Should be set to Level 1 or 2>***

`transfermode= uits` ***<Should always be uits>***

END OF STEPS

□

Set Up TCP/IP Communication on the Metropolis™ DMX

Purpose This procedure is used to enable a TCP/IP LAN connection on the Metropolis™ DMX using the Metropolis™ DMX CIT.

Before you begin Verify that the Metropolis™ DMX is connected to the J16 port on the rear panel of the system using an RJ 45 connector.

You will be required to log in to the CIT. The default login is ***LUC01***; the default password is ***DMX2.510G***. The backup default login is ***LUC02***; the backup default password is ***DMX2.510G***.

Task Complete the following steps to enable the LAN connection for an Metropolis™ DMX using the CIT.

1 Log into the CIT using the CIT default logins and passwords.

2 Enter the `ACT-USR` command. The command syntax is:

`ACT-USER:TID:LUC01:RSF::DMX25G10G;`

3 Enter the `ENT-IPMAP` and `RTRV-MAP`commands, to set up a Metropolis™ DMX for IP connectivity:

To specify the IP address of the NE, enter:`ENT-IPMAP:DMXTID::CTAG:::TCPIPADDR=xxx.xxx.xxx.xxx,ACID=TL1OTHER1;`

To specify the IP Address of the Navis™ Optical EMS server, enter:`ENT-IPMAP:DMXTID::CTAG:::TCPIPADDR=xxx.xxx.xxx.xxx,TCPIPHOST`

Enter: `RTRV-MAP:TID::RSF;`

END OF STEPS

□

Set Up OSI Communication on the Metropolis™ DMX

Purpose This procedure is used to set up OSI communication on the Metropolis™ DMX using the Metropolis™ DMX CIT.

Before you begin Verify that the Metropolis™ DMX is connected to the J16 port on the rear panel of the system using an RJ-45 connector.

You will be required to log in to the CIT. The default login is ***LUC01***; the default password is ***DMX2.510G***. The backup default login is ***LUC02***; the backup default password is ***DMX2.510G***.

Task Complete the following steps to set up OSI communication for an Metropolis™ DMX NE using the CIT.

1 Log into the network element's CIT using the CIT default logins and passwords.

2 Enter the `ACT-USER` command. The command syntax is:

```
ACT-USER:TID:LUC01:RSF::DMX25G10G;:
```

3 Enter the following `ENT-ULSDCC-L3`commands:

```
ENT-ULSDCC-L3:DMXTID:AID:CTAG:::[SPEC_BLOCK];
```

```
ENT-ULSDCC-L3:DMXTID::CTAG:::L3LV2IS=ENABLE,L3AREA=0000;
```

Where, `SPEC_BLOCK` can be the following:

L3ORG is a 6 digit Organization Number.

L3RES is a 4 digit reserved number.

L3RD is a 4 digit Routing Domain number.

L3AREA is a 4 digit Area number.

L3LV2IS is a Level 2 Routing Enabled/Disabled.

END OF STEPS

□

Set Up TCP/IP Communication on the LambdaXtreme™ Transport

Purpose This procedure is used to configure the LambdaXtreme™ Transport for TCP/IP communication.

Before you begin In this procedure, you will establish two IP addresses. The first IP address, which is assigned automatically, establishes communication between the LambdaXtreme™ TransportCIT and the LambdaXtreme™ Transport. The second IP address—which requires the EMS port address, subnet mask, and default router address—establishes communication between the LambdaXtreme™ Transport and the Navis™ Optical EMS.

Task Complete the following steps to configure a LambdaXtreme™ Transport for TCP/IP communication.

1 Connect an RJ45 straight-through cable to the LAN card in the PC and to the LambdaXtreme™ Transport CIT port on the SIO pack.

2 Verify that the green LED is lit on the SIO, NCTL, and SCTL.

Result:

If a proper LAN connection has been made, the LED on the CIT port should be lit. Go to step 4. If the green LED on the port does not light after 30 seconds, go to step 3.

3 If the green LED on the port does not light, check the RJ45 cable.

4 Double click on the **LambdaXtreme™ Transport CIT Release 1.0** on the desktop or click **Start > Programs > Lucent Technologies > LambdaXtreme™ Transport Release 1.0 > LambdaXtreme™ Transport CIT R1.0** to start the LambdaXtreme™ Transport CIT.

Result:

A `Warning – Legal Notice` is displayed.

5 Read the Warning — Legal Notice.

6 Click **OK** to continue.

Result:

The CIT OLS Manager window opens and an NE icon appears in the main window. **Important!** The DHCP server assigns IP addresses to the NE and to the PC LAN card, if needed. This process can take up to 30 seconds. Once IP addresses are assigned, an icon showing a CIT connected to the LambdaXtreme™ Transport is displayed in the OLS Manager window.

7 Right click the icon for the NE and select **Login**.

Result:

A Login window is displayed.

8 To log in, enter these default values:

`User ID`: `LUC01` or `LUC02` or `LUC03`

`Password`: `LUONG+01` or `LUONG+02` or `LUONG+03`

9 Click **OK**.

Result:

If the login is successful, the Node Manager window of the LambdaXtreme™ Transport CIT is displayed.

10 From the Node Manager window, select **Administration > System**.

Result:

The System Administration window is displayed.

11 Click on the EMS Port tab.

Result:

The EMS Port window is displayed, which allows you to provision the IP address, subnet mask, and default router addresses.

12 At the EMS Port IP Address field, enter the IP address of the NE's EMS port, which is also known as the ***OS port***.

13 At the EMS Subnet Mask field, enter the IP address mask that the NE software uses to route messages within the local subnetwork.

14 At the EMS Default Router IP Address field, enter the IP address of the router that is used for out-going messages from the NE that is targeted outside the local subnetwork.

15 Click **OK**.

Result:

The IP address for communication between the Navis™ Optical EMS and the LambdaXtreme™ Transport is established, but it does not take effect until Navis™ Optical EMS logs back into the NE using this address.

END OF STEPS

□

6 Trouble Clearing

Overview

Purpose This chapter describes procedures that can facilitate troubleshooting problems with software components of Navis™ Optical EMS and its communications interfaces.

Contents

□

Navis™ Optical EMS/Navis™ Optical NMS Interface Troubleshooting

Overview

The Navis™ Optical EMS application supports two Navis™ Optical NMS interfaces:

- The ***server-to-server interface*** passes NE information from the Navis™ Optical EMS to the Navis™ Optical NMS. This interface, which is also referred to as the ***northbound TL1 interface*** and the ***southbound interface***, is a socket connecting the Navis™ Optical NMS server to the Navis™ Optical EMS server.
- The ***GUI-to-GUI interface*** is a cut-through that allows the Navis™ Optical NMS to invoke the Navis™ Optical EMS GUI screens from the Navis™ Optical NMS GUI. Both the Navis™ Optical NMS and Navis™ Optical EMS applications refer to this interface as the ***F-interface***. Both applications must be installed on a Windows NT Terminal Server and be properly configured to communicate. The interface supports a one-to-many configuration where one Navis™ Optical NMS GUI can communicate with many Navis™ Optical EMS GUIs of different versions.

Important! If Navis™ Optical NMS (SONET) does not receive notifications, verify that the local DNS domain name is not set.

GUI-to-GUI interface setup

A configuration file, called *sncFint.cfg*, is delivered with each release of Navis™ Optical EMS—it is identical across all versions of Navis™ Optical EMS software. This file, which defines the operation of the F-interface, is a flat, ASCII text file that can be edited using Notepad. Its configuration parameters are defined as name value pairs. Help text in the file explains the purpose of each configuration parameter.

The configuration parameters defined by this file are:

- The ***debug*** configuration parameter defines whether debugging is enabled for the F-interface. When debugging is enabled, the debug output is captured in the Navis™ Optical NMS output log file. The default debugging parameter configuration file entry is:

  ```
  debug        false
  ```

The valid values are ***true*** and ***false***. The value should be set to ***true*** when the F-interface is not working and more detailed information about the fault is required.

- The ***idleTimeout*** configuration parameter is used to set the idle timeout value expressed in seconds. The default timeout value is 10 minutes. The idle timeout can be disabled by setting the value to 0. The default idle timeout configuration file entry is:

  ```
  idleTimeout        600
  ```

  The idle timeout value of 600 seconds overrides the Navis™ Optical EMS GUI timeout defined on the Global Security Parameter Screen because the F-interface is a resource intensive interface that should not be allowed to remain active as long as an individual Navis™ Optical EMS user login session.

- The ***release*** configuration parameter is used to map the Navis™ Optical EMS software version number to directories containing Navis™ Optical EMS GUI software on a Windows NT Terminal Server. When an EMS is defined in the Navis™ Optical NMS database, the type of EMS is defined and the release number of the EMS software is also defined. When the F-interface is invoked, this release number is used by the F-interface software to find the correct version of the Navis™ Optical EMS GUI software. An ***important note***: these definitions assume that the Navis™ Optical NMS GUI and the Navis™ Optical EMS GUI are located on the same drives (generally C drive).

  Valid release numbers can be any string, but typical strings are in the format of ***R6.0*** or ***R5.1***. The configuration file must define a directory for each release number defined in the Navis™ Optical NMS.

  The default configuration file entries for these mappings are:

  ```
  release  default \emsR2
  release  R10.0   \emsR3
  release  R9.0    \emsR21
  release  R8.0    \emsR2
  ```

The first line defines the GUI software that is used when the F-interface finds an unknown release number. In this example, when a unknown release number is sent via the F-interface, the GUI contained in the *\emsR2* directory is used.

- The ***user*** configuration parameter is used to override the username and password settings for Navis™ Optical EMS login. By default, the user login name for the F-interface is ***itm*** and the password is ***itm+123***. For security, default passwords are not defined in the configuration file. However, if configuration parameter entries are entered in the configuration file, the defined entries override the default values. Valid configuration file entries for username and password are:

```
user itm password
itm 123
```

The path of the default F-interface configuration file is:

<default root directory of Navis™ Optical EMS/Navis™ Optical EMS GUI directory>/ems/fint/sncFint.cfg

For the F-interface to work properly, this file must be accurately configured and a copy of this file MUST be installed in this Navis™ Optical NMS GUI software directory:

/jui/jnm/itm/southbound/snc/sncFint

Navis™ Optical NMS Software Configuration

Since some Navis™ Optical EMS Java™ code runs in the Navis™ Optical NMS JVM, a single instance of the Navis™ Optical EMS GUI must be included in the NM classpath. The Navis™ Optical NMS classpath is defined in the file:

/jui/bin/run_jnm.bat

Generally, the Navis™ Optical NMS is preconfigured to invoke an Navis™ Optical EMS R3 GUI located in the \emsR3 directory. If a Navis™ Optical EMS R3 GUI does not exist in \emsR3 directory on the NT Terminal Server, the Navis™ Optical NMS configuration file will need to be changed.

The typical classpath definition for a Navis™ Optical EMS CLASSPATH in the run_jnm.bat file is:

```
SNMSDIR=%3\emsR10
SNMSPATH=%SNMSDIR%;%SNMSDIR%\jars\swing.jar;%SNMSDIR%\jars
SNMSDIR%\jars\org.jar
```

```
CLASSPATH=<NM Classpath>;%SNMSPATH%
```

□

Check the Status of the Navis™ Optical EMS Application

Purpose

Use this procedure to check the status of the Navis™ Optical EMS application.

Additional Information

If the application is up, the system displays the CURRENT RUN LEVEL (status) as ***Running*** and lists the demon name, process ID (pid), process name, run status (option), and the number of respawns for each application process.

The three CURRENT RUN LEVEL (status) states for the application are the following:

- ***shutdown***, in which the Navis™ Optical EMS application is not up
- ***administrative***, in which the Navis™ Optical EMS application is in transition (coming up or going down)
- ***running***, in which the Navis™ Optical EMS application is up

If the application is in the ***running*** state, the command output displays the process names, which are the following:

- ***EMS:BR_bacres***, which is the NE Backup and Restore Module
- ***EMS:CF_NeAgent***, which is the NE Configuration Module
- ***EMS:CF_NeProxy***, which is the NE Configuration Module Proxy Server
- ***EMS:NT_Manager***, which is the Network Topology Management Module
- ***EMS:CM_Server***, which is the Communications Manager
- ***EMS:SM_Security***, which is the Security Management Module
- ***EMS:FM_Server***, which is the Fault Management Module
- ***EMS:OAM_Scheduler***, which is the Process Scheduling Module
- ***EMS:PM_DC***, which is the Performance Management Module
- ***EMS:PM_FTAM***, which is the Performance Management Module through FTAM
- ***EMS:LM_Logger***, which is the Log Management Module
- ***EMS:SDS_Server***, which is the SONET Directory Service Module

Task Complete the following steps to check the status of the Navis™ Optical EMS application.

1 Log in as `root`.

2 At the UNIX prompt, enter the command `appstat`.

Result:

If the application is up, the system displays the CURRENT RUN LEVEL (status) as ***Running*** and additional information is displayed. Go to steps 3 and 4.

If the application is down, the message `CURRENT RUN LEVEL IS: Shutdown` is displayed.

3 If the application is up, examine the `Respawns` field to verify that it contains a 0 for every process. If any field has a number larger than 0, then that process has terminated and automatically restarted.

4 If the application is up, examine the `Pid` field to verify that it has a number greater than 0 for every process. If any field shows a 0, then that process has terminated and is no longer running. The application must be restarted.

5 To further determine if the process is running and is bound to Orbix, enter the command `psit | more` at the UNIX prompt.

END OF STEPS

□

Check the Status of Stopped Processes

Purpose Use this procedure to check the status of stopped processes. Any process name that is reported has been terminated and is no longer running. The process needs to be restarted either by executing `appstart -n` <process name> or the application must be restarted.

Task Complete the following steps to check the status of stopped processes.

1 Log in as `ems`.

2 At the UNIX prompt, enter the command: `appstx`.

Result:

The system output shows the current run level (application status) and a list any processes, by demon name, that have stopped.

END OF STEPS

□

Check the Communication Status of Managed NEs

Purpose Use this procedure to check the communication status of managed NEs.

Task Complete the following steps to check the communication status of managed NEs

1 Log in as `ems`.

2 At the UNIX prompt, enter the command: `cmtool -a`

Result:

The system output shows the following for each NE: the communications port, the NE TID, a communications active flag (Y=Yes), the communications type, the communications channel ID, the communications link status (Up or Down), and the NE login status (On or Off).

END OF STEPS

□

Activate an NE

Purpose

Use this procedure to activate a network element (NE) using the `cmtool` command.

Related information

For a complete list of `cmtool` features, enter the command `cmtool -l`. The `cmtool` command can provide the status of one or all GNE links or one NE link, activate or deactivate an NE, resynchronize a configuration file, switch to/from primary/backup GNEs, and change an NE password.

cmtool usages:

cmtool [-a] display all NE status

cmtool [-h hostname]

cmtool [-s] option for switch primary/backup GNE with -p -b options

cmtool [-p primary GNE tid] [-b backup GNE tid]

cmtool [-l] list all tool features for select

cmtool [-f functional_index] [-n|g netid [-o op]]

cmtool [-n Netid] display NE status

cmtool [-g Gnetid] display GNE status

cmtool [-c netid] change NE password

cmtool [-o [a|d]] option of activate/deactivate

cmtool [-?] for help

In addition, see "Deactivate an NE" (6-12) for additional information.

Task

Complete the following step to activate an NE.

1 At the UNIX prompt, enter the command `cmtool -n` <***TID***> `-o a`

Result:

The system output indicates that a new NE connection has been made and shows the IP address of the NE.

END OF STEPS

□

Deactivate an NE

Purpose Use this procedure to deactivate a network element (NE) using the `cmtool` command.

Related information See “Activate an NE” (6-11) for additional information.

Task Complete the following step to deactivate an NE.

1 At the UNIX prompt, enter the command `cmtool` -n <***TID***> `-o d`

Result:

The system output indicates that a deactivate process has been invoked and shows the IP address of the NE.

END OF STEPS

□

Check the GUI Client and Queue Information via GUI_PROBE

Purpose

This procedure is used to check the number of GUI clients currently running on the HP host, the user login(s) for each GUI, and information about all queues.

Additional Information

When the GUI_Probe utility is up and running, the `GS>` prompt appears. You can now enter a `?` for a HELP menu that lists all command GUI_Probe command options.

Task

Complete the following steps to check GUI client and queue information.

1 At the UNIX prompt, enter the command:

`GUI_Probe` <***hostname***> `:GUI_SERVER`

Result:

The system output indicates that a connection has been made to the GUI server and the GS prompt is displayed.

2 To get a list of GUI clients, the user logins currently running on the GUI Server, and the IP address of the logged in user ID, enter `clients` at the `GS>` prompt.

3 To show information about all the queues, enter `queues` at the `GS>` prompt.

4 To exit the `GUI_PROBE` program, enter the `exit` command at the GS> prompt.

END OF STEPS

□

Check the Association Status of WaveStar™ OLS 1.6T NEs

Purpose Use this procedure to show the association status of the managed WaveStar™ OLS 1.6T NEs.

Task Complete the following steps to obtain the association status of the managed WaveStar™ OLS 1.6T NEs.

1 At the UNIX prompt, enter the command `sb400goam`.

Result:

The system displays the prompt --->

2

TO...	ENTER...
Show the status of all WaveStar™ OLS 1.6T NEs	`assocstatus`
Show the status of one WaveStar™ OLS 1.6T NE	`assocstatus` ***NE name***
Set the trace level	`trace`
List active transactions	`listtxn`
Shut down communications with NEs	`shutdown`
Set the logcontrol level	`logcontrol`
Report the number of active, confirmed associations	`assocnt`
Abort association	`assocabort`
Set up an association	`assocreq`
Activate watchdog	`watchdog`
Display statistics	`statistics`
Change the state of overload controls	`overload`
Start association request on threads	`assocthread`
Request an association follow by an abort	`assocandabort`

END OF STEPS

Retrieve the Informix Software Version

Purpose

Use this procedure to retrieve the version of Informix currently being run. The Navis™ Optical EMS software uses Informix Dynamic Server Release 7.31.uc3.1 to maintain a relational database.

Before you begin

To execute the command described in this procedure, you must be logged in as the user `informix` or `ems`.

Task

Complete the following step to retrieve the Informix software release version.

1 At the UNIX prompt, enter the command `dbaccess -v`.

Result:

The system displays the Informix software version number and the software serial number.

Each system has a unique software serial number for its location.

END OF STEPS

□

Retrieve Informix Database Locks

Purpose Use this procedure to retrieve the database locks that the Navis™ Optical EMS application are holding on the Informix database.

Before you begin To execute the command described in this procedure, you must be logged in as the user ***ems***.

Task Complete the following steps to retrieve the database locks that the Navis™ Optical EMS are holding on the Informix database.

1 At the UNIX prompt, enter the command `locks`

Important! If some locks persistently appear, the system may be congested. If the situation persists, the Navis™ Optical EMS application may need to be restarted.

Result:

The system displays a three column message. The first column is the number of database locks being held. The next two columns are the PID and process name, respectively, which are holding the locks.

2 To retrieve detailed lock table information, enter the command `tblocks`

Result:

The system displays a two column message. The first column is the table name and the locks being held. The second column shows the number of locks held on the table.

END OF STEPS

□

Check Informix Database Space Usage

Purpose Use this procedure to retrieve the Informix database space usage.

Before you begin To execute the command described in this procedure, you must be logged in as the user `informix` or `ems`.

Task Complete the following steps to check the space usage of the Informix database.

1 At the UNIX prompt, enter the command `onstat -d`.

Result:

The system outputs the current Informix software release version, the dbspaces, and chunk usage information.

2 Verify that the free column for the dbspace partitions is not approaching 0.

Result:

If it is approaching 0, the database is running out of free space. Proceed to steps 3 and 4.

If it is not approaching 0, the procedure is complete.

3 Use `add_dbs dbspacename` to add additional 10M to the dbspace specified. (The application does not have to be brought down to add dbspace.)

4 Reissue the `onstat -d` command to verify that the dbspace partitions have been increased to the proper size.

END OF STEPS

□

Check Informix Error Codes

Purpose Use this procedure to display Informix error codes and their associated text.

Before you begin To execute the command described in this procedure, you must be logged in as the user `informix` or `ems`.

Task Complete the following step to display Informix error codes and associated text.

1 At the UNIX prompt, enter the command `finderr xxx`

where `xxx` is the specific Informix error code.

Result:

The system displays output indicating the Informix error code, the error code message text, and a brief statement about the possible solution to the error.

END OF STEPS

□

Monitor the OSI Stack on an HP Server

Purpose Use this procedure to monitor the OSI stack on an HP server. Once the `osiopu` process is running, you can send TARP requests to NEs.

Task Complete the following steps to monitor the OSI stack on the HP server.

1 At the UNIX prompt, enter the command `osiopu`.

Result:

System messages indicate that the `osipu` process has started and a UNIX prompt is returned.

2

TO...	ENTER THE COMMAND...
Send a TARP request to a specific NE	`tarp getnsap C` *<TID>* **Important!** An important complimentary command to the `tarp getnsap C` command is: `tarp gettid H` . It productes the NASP of the NE for which you would like the TID. If output from the completed TARP request obtained from isssuing the above command shows that the origin is from TDC, flush the TDC cache.
Flush the TDC cache	`tarp tdc flush`

3 To exit the `osiopu` command session, enter `$exit`.

Important! You must exit the `osipu` session before bringing the Navis™ Optical EMS down and then up, or problems can occur.

END OF STEPS

□

Verify IP Addresses and Names

Purpose

Use this procedure to verify network device IP addresses and names for the Navis™ Optical EMS server and workstations.

Related information

Hosts and other network devices that are in the same physical location are either connected via 10BaseT unshielded twisted pair cables through a hub or they are connected to each other directly by coaxial cable.

Network devices that are not at the same location are connected over T1 lines using Channel Service Units/Data Service Units (CSU/DSUs) and routers.

Each line of the */etc/hosts* file contains an IP address and name for systems on the same network. All Navis™ Optical EMS system names must be six characters or less, and begin and end with a letter.

Task

Complete the following step to verify network IP addresses and names for systems on the same network.

1 At the UNIX prompt, enter the command `cat /etc/hosts | pg`.

Result:

The system displays the contents of the */etc/hosts* file.

END OF STEPS

□

Test LAN Connectivity

Purpose Use this procedure to check IP connectivity to other devices on the same network.

Task Complete the following steps to check IP connectivity to other devices on the same network.

1 Log into the host system as `ems`.

2 At the UNIX prompt, enter the command `cat /etc/hosts | pg`

Result:

The system displays the contents of the */etc/hosts* file. Each line contains an IP address and name for systems on the same network.

3 Note the name of the host, workstation, or device to be tested.

4 At the UNIX prompt, enter the command `/etc/ping` *`name`*

where *`name`* is the *`name`* of the device to be tested for connectivity.

Wait a few seconds for the system to transmit and retransmit packets of data to/from remote workstations.

5 Press Control **C** to stop the test.

END OF STEPS

□

Test Twisted Pair Wiring

Purpose Use this procedure to test network devices that use twisted pair wiring. Follow this procedure if the router responds positively and the workstation does not respond.

Before you begin Check the following possibilities for networks that use twisted-pair wiring:

- Devices are powered off or unplugged.
- Loose connections or broken wires between the workstation and hub or hub and router.

Try pinging the workstation using the procedure “Test LAN Connectivity” (6-21). If pinging the workstation still fails, follow this procedure.

Task Complete the following steps to test network devices, such as a workstation, that use twisted-pair wiring.

1 Reboot the workstation.

2 Log in to the workstation.

3 At the UNIX prompt, enter the command `/etc/reboot`

4

IF...	THEN...
Pinging the workstation still fails	Try rebooting both the router and hub by turning them off and back on.
Trouble still persists	Try replacing wiring and swapping out the hub.

END OF STEPS

□

Test Stations Connected Via Coaxial Cable

Purpose Use this procedure to test network devices connected via coaxial cable.

Before you begin Check the following possibilities for networks that use coaxial cable:

- Devices are powered off or unplugged
- AUIs are loosely connected
- Cables between nodes are improperly connected or non-terminated

Task Complete the following steps to test network devices, such as a workstation, that use coaxial cable.

1 Ping the workstation using the "Test LAN Connectivity" (6-21) procedure.

Result:

If pinging the workstation fails, go to step 2.

2 Reboot the workstation and the router.

Result:

If the trouble still persists after rebooting the workstation and the router, go to step 3.

3 Try swapping AUIs and replacing cables.

END OF STEPS

□

Test Navis™ Optical EMS to Navis™ Optical NMS Cut-Through

Purpose Use this procedure to test the Navis™ Optical EMS-to-Navis™ Optical NMS cut-through interface.

Task Complete the following steps to test the Navis™ Optical EMS-to-Navis™ Optical NMS cut-through interface.

1 Log into Navis™ Optical NMS and go to the Navis™ Optical NMS controllers map.

2 Place the mouse cursor over the center of the Navis™ Optical EMS icon.

3 Click the mouse button that brings up the pop-up menu.

4 Select the VCIT menu item via the cascading menus:

Session->Virtual Craft Interface Terminal

5

IF...	THEN...
The Navis™ Optical NMS GUI is not working	Invoke the Navis™ Optical EMS GUI by using telnet to log into the Navis™ Optical EMS server, change the directory to the Navis™ Optical EMS GUI software directory, and enter the command `[ems -host <hostname> -nobs -up itm itm+123`

6

IF	THEN
The login is successful	Proceed to step 10

IF	THEN
If the login is unsuccessful	Check the password of the ITM login. If the password is not ***itm+123***, it might be ***itm123***. If you need to define an ITM password that is NOT ***itm+123***, edit the configuration file to override the default ITM password for the F-interface. If the GUI displays an error indicating that the `EMS is not running`, log into the HP server and execute the command: `appstat`

7

IF	THEN
The Navis™ Optical EMS application not running	Bring up the Navis™ Optical EMS application by entering the command `up`
The Navis™ Optical EMS application is already up and running	Enter the command psit | grep GUI_Server If a message is displayed indicating that the GUI server is running, the application is running

8

IF...	THEN...
The Navis™ Optical EMS application is running but there are still problems	The Navis™ Optical NMS host is using a host name that is mapping to the wrong Navis™ Optical EMS server IP address. Check the IP addressing in the file ***M:{Winnt|Wtsrv}\system32\drivets\etc\hosts***

9

IF...	THEN...
There was no command output messages displayed from running the `psit` command in Step 7	Restart the GUI_Server process by entering the command `apprestart -n GUI_Server` Once the `apprestart` command is complete, retry the command psit | grep GUI_Server

10 Check the Navis™ Optical NMS batch file for the correct Navis™ Optical EMS classpath.

11 Edit the file */jui/bin/run_jnm.bat* so the Navis™ Optical EMS classpath is defined for each Navis™ Optical NMS CLASSPATH definition.

12 Check the F-interface configuration file to determine if each release in the configuration file maps to the correct GUI software directory. The F-interface configuration file is:

/jui/jnm/itm/southbound/ems/emsFint/emsFint.cfg.

13 Make any necessary edits to the F-interface configuration file.

14 Try again to launch the Navis™ Optical NMS interface via the controllers map and the VCIT menu item.

Result:

If the cut-through still fails, go to the next step. If the cut-through does not fail, then the procedure is complete.

15 If the cut-through continues to fail, access the Navis™ Optical NMS debug log file. The filename of the debug log is displayed at Navis™ Optical NMS startup time and the file is always located in the */jui/logs* directory. **Note:** If you examine the log immediately after the cut-through failure, the debug output be near the end of the file.

16 Check the debug log file for the following:

- Determine whether the software found the configuration file.
- Determine whether the correct GUI software was launched for the specified Navis™ Optical EMS host.

Note: Unless a new bug emerges in the software, the problem is always the result of the wrong version of Navis™ Optical EMS GUI software being launched.

END OF STEPS

□

7 Cluster Administration GUI Operations

Overview

Purpose

This chapter provides general information about the cluster administration GUI, which is a GUI that is used to monitor geographically redundant HP servers and to perform switchovers between HP servers, as necessary. This chapter also provides the procedures related to the HP cluster administration GUI.

Contents

□

The Cluster Administration GUI

Introduction

The Navis™ Optical EMS architecture supports high availability through three levels of redundancy:

- ***Basic Host Redundancy*****—**redundant components are available in a single computer. Recovery relies on switching control to another resource on the same host such as a backup LAN card or mirrored disk.
- ***Local Redundancy*****—**the HP server is supported by a similarly equipped, redundant host located in the same building. If the primary host fails, the backup host is activated automatically without user intervention.
- ***Geographic Redundancy*****—**a primary Navis™ Optical EMS host or server is supported by a similarly equipped, redundant host located in a physically different location. If the primary host fails, the backup host is activated via manual operation.

Navis™ Optical EMS has a cluster administration GUI that allows an administrator to monitor redundant HP servers. The cluster administration GUI provides information on the current cluster status and allows an administrator to perform geographic site switchover on demand. An automatic switchover between the primary HP server and a geographically remote, redundant HP server can also be set up through the cluster administration GUI.

The cluster administration GUI is distinct from the Navis™ Optical EMS GUI; and except for the login, neither GUI shares any common functionality.

□

Geographic Redundant Configurations

Overview

Geographic redundancy employs up to two similarly equipped hosts located in different geographic locations (for example: New York and London). Each host is configured with redundant hardware components and supports data replication of the Navis™ Optical EMS database.

The cluster administration GUI supports a 1+1 geographic redundant configuration.

1+1 configuration

In a 1+1 configuration, a single redundant Navis™ Optical EMS server is located in two separate locations. In the normal operating mode, the primary Navis™ Optical EMS server is active and runs the EMS application. The other Navis™ Optical EMS server is a ***warm*** standby and is running the EMS application in ***read only*** mode.

Geographic failover between the active and standby host can be performed on demand from either of the following:

- cluster administration GUI
- command lines of the standby and active servers

To make the remote station's server active, the cluster administration GUI can be used to perform a manual or automatic switchover.

Failure recovery

When a switchover occurs, the EMS application on the previously active Navis™ Optical EMS server is shutdown. During shutdown, the Navis™ Optical EMS server is no longer participating in the automatic data replication services. Therefore, before being restored to service, the Navis™ Optical EMS application database on the shutdown host must resynchronized with the active Navis™ Optical EMS server. For details, see the *Navis™ Optical EMS Installation Guide*.

Once fully synchronized and the application is restarted, a manual switchover can be made to revert service to the server.

□

The Cluster Administration GUI

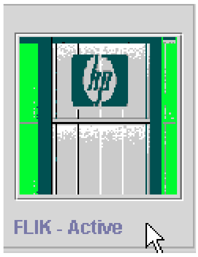
Overview

The Cluster Administration GUI is a simple GUI that monitors the health of the HP servers in the cluster. The GUI main window displays the two geographically separated stations, labeled local and remote, with each host contained therein.

HP server icons

Each HP server is represented on the cluster administration GUI by an icon, which is illustrated in the following two figures.

Figure 7-1 Figure 1 - Operational Navis™ Optical EMS Server Icon

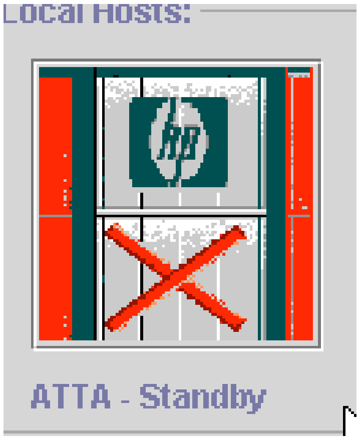


A label just underneath the server icon displays the name of the server and the server's role in the cluster. The two valid cluster roles are:

Label	Meaning
Active	The associated HP server is the active server in the cluster. The EMS application on this server is responsible for performing all NE management operations.
Standby	The associated HP server(s) are acting as warm standby(s) for the currently active server. The associated EMS application(s) are running in read only mode.

When the cluster administration GUI loses communication with a HP server in the cluster, it marks the server as failed and changes its color to red. A failed server also has an ***X*** through the center of its icon; see the following figure. The server is marked as failed until communication is re-established to the server.

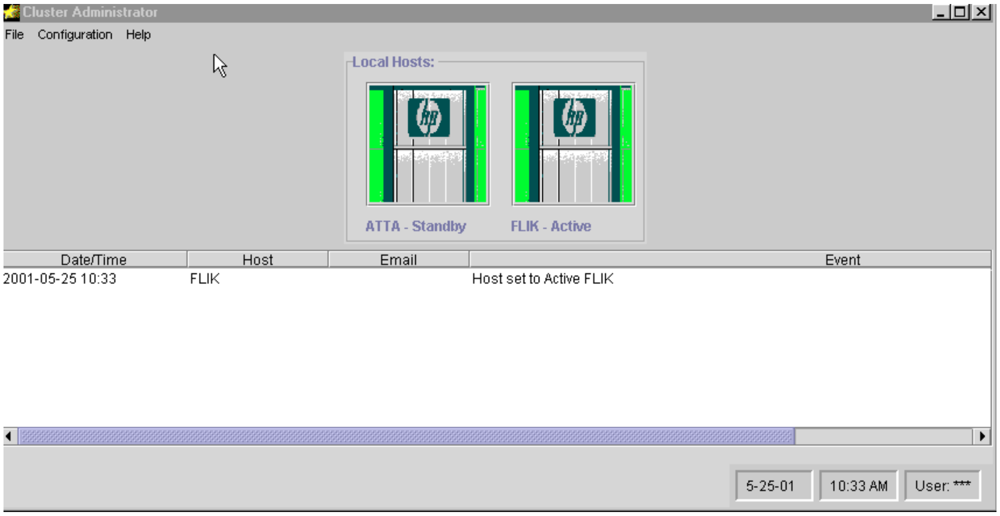
Figure 7-2 Failed Navis™ Optical EMS Server Icon



Cluster administration GUI Main Window

The following figure shows an example of the cluster administration GUI Main Window Administration window for a 1+1 configuration.

Figure 7-3 Cluster Administration GUI Main Window (1+1 Configuration)



Date/Time	Host	Email	Event
2001-05-25 10:33	FLIK		Host set to Active FLIK

□

Cluster Administration GUI Features

Email and user configuration

The cluster administration GUI will send email and/or page a set of users when any of the following conditions occur:

- any HP server in the cluster fails (in other words, stops communicating on the LAN)
- a failover is initiated through the GUI
- an automatic switchover is performed by the GUI

In addition, the HP server can also send email messages when a failure or abnormal condition is detected. In each case, the messages that are sent to the user are hard coded strings that indicate:

- the reason for the email/page
- the source of the email/page (in other words, the HP server or the cluster administration GUI)
- the affected HP server

The users, who receive email and/or a page, whether from the HP server or the cluster administration GUI, are defined through the cluster administration GUI. The Manage Email Information window is reached from the menu bar on the cluster administration GUI Main window by choosing **Configuration** and then by choosing **Email Addresses** from the Configuration sub-menu.

Adding, modifying, deleting, and viewing user email accounts requires a valid password for the user `itm`. User validation is performed on any server that has a running EMS application. Once the GUI user is validated, the Manage Email Information window is displayed.

The Manage Email Information window displays the name of all users who receive email. There is no limit to the number of users who can be added to the list. The following operations can be performed from this window:

- add a new user to receive email notifications
- delete a user from the list of users receiving email notifications
- modify user email/pager information
- view user email/pager information
- test email/pager information for a specific user

Users who receive email are completely unrelated to the Navis™ Optical EMS GUI application users, managed by the Navis™ Optical EMS application Security feature.

Automatic switchover configuration

The cluster administration GUI can be configured to perform automatic switchover when the GUI detects a failure.

Manual switchover

The cluster administration GUI provides two methods to perform a manual switchover:

- Press the Navis™ Optical EMS server icon button on the main window.
- Request a site switchover from the menu bar on the cluster administration GUI Main window.

Performing a manual switchover requires a valid password for the `itm user` account. User validation is performed on any server that has a running EMS application.

Security

Most operations on the cluster administration GUI require the user to validate himself or herself as a Navis™ Optical EMS user. Validation consists of ***logging in*** to the cluster administration as the user `itm`.

Unlike the login for the regular Navis™ Optical EMS GUI, the cluster administration GUI does not register a logged in user with any HP server running the Navis™ Optical EMS application. Instead, the `itm` user password is validated through the security process of any communicating HP server running the application. If the password is valid, the user is considered authenticated and permission to perform cluster administration GUI operations is granted. However, a corresponding server login does not exist for the account.

The user is logged in to the cluster administration GUI when the `itm` user ID is displayed in the user text field on the bottom, right corner of the main window. If the user is not logged in, `***` is displayed in the user text field. The user is requested to log in the first time an operation, which requires login privileges, is executed. From that point, the user remains logged in until the user logs out or the cluster administration GUI terminates.

□

Start the Cluster Administration GUI

Purpose Use this procedure to start the cluster administration GUI.

Task Complete the following steps to start the cluster administration GUI.

1 Log into the client workstation.

2 Change directory to the Navis™ Optical EMS GUI home directory on the client workstation (for example, loaded with Navis™ Optical EMS Release 8.0).

IF...	ENTER...
It is a Windows-based system	`cd \emsR8.0`
It is a UNIX-based system	`cd <emsR8.0 home directory>`

3 Execute the cluster launch script, indicating the name of a single (any) HP server in the cluster.

IF...	ENTER...
It is a Windows-based system	`CLUSTER -host <ems host name>`
It is a UNIX-based system	`cluster.sh -host <ems host name>` **Result:** A Login window is displayed.

4 Enter the user login `itm`.

Important! You are only prompted for a login if you execute a menu item. By default, the system displays the main window.

5 Enter a valid password for user login `itm`.

6 Click the OK button.

Result:

The cluster administration GUI Main window is displayed.

END OF STEPS

□

Stop the Cluster Administration GUI

Purpose Use this procedure to stop the cluster administration GUI.

Task

1 From the menu, select **File > Exit**.

Result:

The GUI window is removed from the screen.

END OF STEPS

□

Configure Mail Server

Purpose Use this procedure to configure the cluster administration GUI's email server.

Before you begin You must start up and log into the cluster administration GUI.

The email server configuration only applies to the client workstation running the cluster administration GUI. If more than one client workstation is running the cluster administration GUI, each client workstation needs to be appropriately configured.

Related task "Start the Cluster Administration GUI" (7-9)

Task Complete the following steps to configure the cluster administration GUI email server.

1 Choose **Configuration** from the menu bar on the cluster administration GUI Main window.

Result:

The Configuration sub-menu is displayed.

2 Choose **Mail Server** from the Configuration sub-menu.

Result:

The Edit Mail Server window is displayed. If you are not logged in, you will be prompted for your login password.

3 Enter the name of the GUI's mail server.

4 Click the OK button.

Result:

The mail server is defined for routing email.

END OF STEPS

□

Add a New Email User

Purpose

Use this procedure to add a new user email account for the cluster administration GUI.

Before you begin

You must start up and log into the cluster administration GUI.

The list of email users is saved on the active server and then replicated to all standby servers. Therefore, email user information, retrieved for the Manage Email Information window, is retrieved from any communicating HP server running the Navis™ Optical EMS. However, when saving new email information, new email user information is only saved on the active server. If the active server is not communicating, adding a new email user is not permitted.

Related task

"Start the Cluster Administration GUI" (7-9)

Task

Complete the following steps to add a new user email account.

1 Choose **Configuration** from the menu bar on the cluster administration GUI Main window.

Result:

The Configuration sub-menu is displayed.

2 Choose **Email Addresses** from the Configuration sub-menu.

Result:

The Manage Email Information window is displayed. At this time, you will be prompted for a login and password if you have not supplied one already.

3 At the prompt, supply a login and password if you have not already done so.

4 Click the Add button on the Manage Email Information window.

Result:

The Email Account Information window is displayed.

5 Under **User Name**, enter the user name for the new email user. Any ***unique*** value may be entered for this field.

6 Enter information for only one of the following:

- Email Address—Enter an email address to which mail for this user can be sent.
- Pager Address—An email address to which pager mail for this user can be sent. This field is optional.

7 After entering the field information, click the Apply button to create the new email user account and leave the window open, or click the OK button to create the new email user account and close the window.

8 Click the OK button.

Result:

The Status Dialog window is displayed, which indicates that the user is being added to Navis™ Optical EMS.

END OF STEPS

□

Modify User Email Information

Purpose Use this procedure to modify user email account information for the cluster administration GUI.

Before you begin You must start up and log into the cluster administration GUI.

Related tasks

- “Start the Cluster Administration GUI” (7-9)
- “Add a New Email User” (7-13)

Task Complete the following steps to modify user email information.

1 Choose **Configuration** from the menu bar on the cluster administration GUI Main window.

Result:

The Configuration sub-menu is displayed.

2 Choose **Email Addresses** from the Configuration sub-menu.

Result:

The Manage Email Information window is displayed. If you are logged in, go to step 4. If you are not logged in, you will be prompted for your login password. Go to the next step.

3 If you are not logged in, supply a login and password.

4 Double-click to select a user from the user list.

5 Click the Modify button.

Result:

The Email Account Information window is displayed.

6 Change the User Name, Email Address, and/or Pager Address fields, as required.

7 Click the Apply button to save your changes and leave the window open, or click the OK button to save your changes and close the window.

END OF STEPS

□

Delete User Email Information

Purpose Use this procedure to delete a user's email information from the cluster administration GUI.

Before you begin You must start up and log into the cluster administration GUI.

Related tasks

- "Start the Cluster Administration GUI" (7-9)
- "Add a New Email User" (7-13)
- "Modify User Email Information" (7-15)

Task Complete the following steps to delete a user's email information.

1 Choose **Configuration** from the menu bar on the cluster administration GUI Main window.

Result:

The Configuration sub-menu is displayed.

2 Choose **Email Addresses** from the Configuration sub-menu.

Result:

The Manage Email Information window is displayed. If you are logged in, go to step 4. If you are not logged in, you will be prompted for your login password. Go to the next step.

3 If you are not logged in, supply a login and password.

4 Double-click to select a user from the user list.

5 Click the Delete button. A pop-up window is displayed, asking if you really want to delete the user's email information.

6 Choose `Yes` to delete the user's email information.

END OF STEPS

□

View User Email Information

Purpose Use this procedure to view a user’s email information for the cluster administration GUI.

Before you begin You must start up and log into the cluster administration GUI.

Related tasks

- “Start the Cluster Administration GUI” (7-9)
- “Add a New Email User” (7-13)
- “Modify User Email Information” (7-15)
- “Delete User Email Information” (7-17)

Task Complete the following steps to view a user’s email information.

1 Choose **Configuration** from the menu bar on the cluster administration GUI Main window.

Result:

The Configuration sub-menu is displayed.

2 Choose **Email Addresses** from the Configuration sub-menu.

Result:

The Manage Email Information window is displayed. If you are logged in, go to step 4. If you are not logged in, you will be prompted for your login password. Go to the next step.

3 If you are not logged in, supply a login and password.

4 Double-click to select a user from the user list.

5 Click the View button.

Result:

The Email Account Information window is displayed, showing the selected user’s email account information.

6 Click the Cancel button to close the Email Account Information window.

END OF STEPS

□

Test User Email Information

Purpose

Use this procedure to test a user's email address on the cluster administration GUI.

Test email messages can be sent from the GUI or the Navis™ Optical EMS server.

Email is sent from the cluster administration GUI when a server failure is detected or an automatic failover occurs, which, in this case, the cluster administration GUI contacts its designated mail server and requests delivery of email to each user on the user email list.

Email is sent from the HP server when the server software detects an abnormal condition in the cluster, which, in this case, the Navis™ Optical EMS software uses the co-resident HP-UX mail server to forward mail to each user on the user email list.

Before you begin

You must start up and log into the cluster administration GUI.

Related tasks

- "Start the Cluster Administration GUI" (7-9)
- "Add a New Email User" (7-13)
- "View User Email Information" (7-19)

Task

Complete the following steps to test a user's email address.

1 Choose **Configuration** from the menu bar on the cluster administration GUI Main window.

Result:

The Configuration sub-menu is displayed.

2 Choose **Email Addresses** from the Configuration sub-menu.

Result:

The Manage Email Information window is displayed. If you are logged in, go to step 4. If you are not logged in, you will be prompted for your login password. go to the next step.

3 Double click to select a user from the user list.

4 Click the TEST button.

Result:

The Email Test window is displayed, with the user's email information along with a sample email subject and a text message that can be edited.

5

TO...	DO THIS...
Send a test message from the client workstation (GUI)	Click the GUI radio button. **Important!** To send a test message from the GUI, you must have a mail server configured correctly. See "Configure Mail Server."
Send a test message from the HP server	Click the HP server radio button.

6 Click the SEND button to send the test email message.

Result:

The system displays a message indicating that the message was sent successfully.

END OF STEPS

□

Enable Automatic Switchover

Purpose

Use this procedure to enable automatic switchover.

The cluster administration GUI can be configured to enable automatic switchover when the GUI detects a failure condition.

If automatic switchover is enabled and the cluster administration GUI detects that a failure condition, warranting a server switchover has occurred, an automatic switchover dialog box is displayed on the GUI, indicating that an automatic switchover is about to be performed.

The dialog box is displayed for the specified elapsed time period. If the failure condition clears while the dialog box is displayed, the dialog box closes and automatic switchover monitoring is resumed. If the failure condition does not clear within the specified elapsed time period, the dialog box is closed, the switchover is performed, and an email is sent informing all users on the email list of the switchover.

The failure elapsed time is the amount of time, after a failure is detected, that elapses before an automatic switchover is performed by the cluster administration GUI. This time allows for intermittent network problems to clear before a switchover is performed. The default value is 10 minutes.

Before you begin

You must start up and log into the cluster administration GUI as user `itm` with a valid password.

Only a single cluster administration GUI should be configured with automatic switchover enabled. However, if two GUIs are enabled for automatic switchover, the second switchover request to the standby HP server would be denied, because a switchover operation would already be in progress.

In step 4, you must configure a failure elapsed time, which is the amount of time after a failure is detected that elapses before the cluster administration GUI performs an automatic switchover. This time allows for intermittent network problems to clear before a switchover is performed. The default value is 10 minutes.

Task

Complete the following steps to set up automatic switchover.

1 Choose **Configuration** from the menu bar on the cluster administration GUI Main window.

Result:

The Configuration sub-menu is displayed.

2 Choose **Automatic Switch Over** from the Configuration sub-menu.

Result:

The Edit Automatic Switchover window is displayed.

3 To enable automatic switching, choose **Enable** from the option menu.

4 Enter a failure elapsed time. The default value is 10 minutes.

5 Click the OK button.

Result:

Automatic switching is now enabled.

END OF STEPS

□

Disable Automatic Switchover

Purpose Use this procedure to disable automatic switchover.

Before you begin You must start up and log into the cluster administration GUI as user `itm` with a valid password.

Task Complete the following steps to disable automatic switchover.

1 Choose **Configuration** from the menu bar on the cluster administration GUI Main window.

Result:

The Configuration sub-menu is displayed.

2 Choose **Automatic Switch Over** from the Configuration sub-menu.

Result:

The Edit Automatic Switchover window is displayed.

3 To disable automatic switchover, choose **Disable** from the option menu, which is the default.

4 Click the OK button.

Result:

Automatic switchover is now disabled.

END OF STEPS

□

Perform Manual Switchover

Purpose

Use this procedure to perform a manual switchover from one server to another if a failure occurs.

Before you begin

Start up and log into the cluster administration GUI as `user itm` with a valid password. This task must be performed from the cluster administration GUI Main window.

Related task

"Start the Cluster Administration GUI" (7-9)

Task

Complete the following step to perform a manual switchover.

1

TO...	DO THIS...
Perform a manual switchover using the HP server icon buttons	Click the Navis™ Optical EMS host icon to be activated. (Each host icon is a button that allows you to initiate a manual switchover to the host.)
Perform a manual switchover from the Main window menu	Choose **Configuration** from the menu bar, then choose **Site Switch Over** from the displayed sub-menu. **Result:** If a switchover operation cannot be performed, an error message is displayed. If the switchover was done using the server icon, the system prompts with a request to verify the switchover operation. Choose Yes to confirm the switchover. If the switchover was performed from the Main window menu, the system discovers the server that is eligible for the switchover. The system prompts with a request to verify the switchover operation. Choose Yes to confirm the switchover.

END OF STEPS

□

Appendix A: Available Functions/T1 Commands

Available Functions/TL1 Commands

Authorization Level 1: Maintenance

The **TL1 Commands Available for Authorization Level 1, Maintenance Functional Category** include the following commands:

RTRV-SNC_ALMCMS

RTRV-SNC_ALM-E1

RTRV-SNC_ALM-E4

RTRV-SNC_ALM-OC192

RTRV-SNC_ALMOCHAN

RTRV-SNC_ALM-OLINE

RTRV-SNC_ALM-OTPS

RTRV-SNC_ALM-OPS

RTRV-SNC_ALM-STM1

RTRV-SNC_ALM-STM1E

RTRV-SNC_ALM-STM4

RTRV-SNC_ALM-STM16

RTRV-SNC_ALM-STM64

RTRV-SNC_ALM-SUPR

RTRV-SNC_ALM-VC3

RTRV-SNC_ALM-VC4

RTRV-SNC_ALM-VCRRC

RTRV-SNC_ALM-ALL

RTRV-EMS_ALM-EQPTR

RTRV-EMS_ALM-COM

RTRV-EMS_ALM-STS12C

RTRV-EMS_ALMSTS12

RTRV-EMS_ALMSTS3C

RTRV-EMS_ALM-STS3

RTRV-EMS_ALM-STS1

RTRV-EMS_ALM-VT1

RTRV-EMS_ALM-OC1

RTRV-EMS_ALM-OC3

RTRV-EMS_ALM-OC12

RTRV-EMS_ALM-T1

RTRV-EMS_ALM-TE

RTRV-EMS_ALM-EC1

RTRV-EMS_ALM-OC48

RTRV-EMS_ALM-OVTG

RTRV-EMS_ALM-FFP

RTRV-SNC_ALM-FOP

RTRV-SNC_ALM-COM

RTRV-SNC_ALM-STS12C

RTRV-SNC_ALM-STS12

RTRV-SNC_ALM-STS3C

Authorization Level 1: Provision

The **TL1 Command Available for Authorization Level 1, Provision (P) Functional Category** is the following:

RTRV-SNC_ASSOC-OTPS

Authorization Level 1: Performance

The **TL1 Commands/Functions are NOT Available for Authorization Level 1, Performance Management (PM) Functional Category**.

Authorization Level 1: Security

The **Functions Available for Authorization Level 1, Security (S) Functional Category** include the following:

SAVE POSITIONS PREFERENCES

SAVE POSITIONS

SAVE PREFERENCES

RESTORE POSITIONS PREFERENCES

RESTORE POSITIONS

RESTORE PREFERENCES

COPY POSITIONS

COPY PREFERENCES

PRINT MAP

USER PREFERENCES

ALL ADMINISTRATION FUNCTIONS

ALL SECURITY

CHANGE PASSWORD

VIEW LOGS

VIEW ALL CMDRSP LOGS

Authorization Level 1: Test Access

TL1 Commands/Functions are NOT Available for Authorization Level 1, Test Access Management (TA) Functional Category.

Authorization Level 2: Maintenance

The **Functions available for Authorization Level 2, Maintenance (M) Functional Category** are the following:

VIEW ALARM MONITORING STATISTICS

ALL ALARM MONITORING STATISTICS

TL1 BROADCAST

TL1 MACRO BUILDER

CUT-THROUGH

Authorization Level 2: Provision

The **TL1 Commands/Functions available for Authorization Level 2, Provision (P) Functional Category** are the following:

RTRV-EMS_CRS-STS1

RTRV-EMS_CRS-STRS12

RTRV-EMS_CRS_STS12C

RTRV-EMS_CRS-STS3C

RTRV-EMS_CRS-STS3

RTRV-EMS_CRS-VT1

RTRV-SNC_CRS-STS12C

RTRV-SNC_CRS-STS3C

RTRV-SNC_CRS-STS3

RTRV-SNC_CRS-STS1

RTRV-SNC_CRS-VT1

RTRV-SNC_INV

RTRV-EMS_INV

RTRV-EMS_NELIST

RTRV-SNC_NELIST

RTRV-EMS_LINKLIST

RTRV-SNC_LINKLIST

TL1 MACRO SCRIPTS, TL1 BROADCAST

TL1 MACRO BUILDER, CUT-THROUGH

VIEW CROSS CONNECT

ALL CROSS CONNECTS

VIEW CROSS CONNECT EQUIPMENT

VIEW PATH

Authorization Level 2: Performance Management

The **Functions available for Authorization Level 2, Performance Management (PM) Functional Category** are the following:

TL1 MACRO SCRIPTS

TL1 BROADCAST

TL1 MACRO BUILDER

CUT-THROUGH, ALL PM

VIEW PM DATA

Authorization Level 2: Security

The **Functions available for Authorization Level 2, Security (S) Functional Category** are the following:

COPY POSITIONS

COPY PREFERENCES

MOVE NODE

RESTORE MAP SETTINGS

RESTORE POSITIONS

RESTORE PREFERENCES

SAVE MAP SETTINGS

SAVE POSITIONS

SAVE PREFERENCES

VIEW ALL CMDRSP LOGS

VIEW LOGS

Authorization Level 2: Test Access

The **Functions available for Authorization Level 2, Test Access (T) Functional Category** are the following:

LIST LOOPBACKS

LIST TEST ACCESS

Authorization Level 3: Maintenance

The **Functions available for Authorization Level 3, Maintenance (M) Functional Category** are the following:

FILTER ALARMS

RESYNCHRONIZE ALARMS

ALARM PROVISIONING

ALW-SNC_MSG-ALL

INH-SNC_MSG-ALL

Authorization Level 3: Provision

The **TL1 Commands/Functions available for Authorization Level 3, Provision (P) Functional Category** are the following:

DLT-EMS_CRS-STS12C

DLT-EMS_CRS-STS1

DLT-EMS_CRS-STS3

DLT-EMS_CRS-STS3C

DLT-EMS_CRS-T1

DLT-EMS_CRS-T3

DLT-EMS_CRS-VT1

DLT-SNC_CRS-STS12

DLT-SNC_CRS-STS12C

DLT-SNC_CRS-STS1

DLT-SNC_CRS-STS3

DLT-SNC_CRS-STS3C

DLT-SNC_CRS-T1

DLT-SNC_CRS-T3

DLT-SNC_CRS-VT1

ED-EMS_EC1

ED-EMS_OC12

ED-EMS_OC3

ED-EMS_OC48

ED-EMS-OVTG

ED-EMS_STS12C

ED-EMS-STS1

ED-EMS_STS3

ED-EMS_STS3C

ED-EMS_T1

ED-EMS_T3

ED-EMS_VT1

ED-SNC_EC1

ED-SNC_OC12

ED-SNC_OC3

ED-SNC_OC48

ED-SNC_OCHAN

ED-SNC_OTPS

ED-SNC_OVTG

ED-SNC_STS12C

ED-SNC_STS1

ED-SNC_STS3

ED-SNC_STS3C

ED-SNC_T1

ED-SNC_T3

ED-SNC_VT1

ENT-EMS_CRS-STS12C

ENT-EMS_CRS-STS1

ENT-EMS_CRS-STS3

ENT-EMS_CRS-STS3C

ENT-EMS-CRS-T1

ENT-EMS_CRS-T3

ENT-EMS_CRS-VT1

ENT-SNC_CRS-STS1

ENT-SNC_CRS-STS12

ENT-SNC_CRS-STS12C

ENT-SNC_CRS-STS3

ENT-SNC_CRS-STS3C

ENT-SNC_CRS-T1

ENT-SNC_CRS-T3

ENT-SNC_CRS-VT1

ADD CROSS CONNECT

ADD PATH

COPY PATH

CREATE OPTICAL ASSOCIATION

DELETE CROSS CONNECT

DELETE OPTICAL ASSOCIATION

DELETE PATH

MANUAL DNO

MODIFY CROSS CONECT

MODIFY OPTICAL ASSOCIATION

MODIFY PATH

PROVISION EQUIPMENT

PROVISION NE

PROVISION PORT

PROVISION PROTECTION GROUPS

Authorization Level 3: Performance

TL1 Commands/Functions are NOT available for Authorization Level 3, Performance Management (P) Functional Category.

Authorization Level 3: Security

The **Functions available for Authorization Level 3, Security (S) Functional Category** are the following:

AUTO DNO

AUTO DTSYNC

BACKUP NE

MANUAL DNO

MANUAL DTSYNC

SCHEDULE BACKUP

SCHEDULE DNO

SCHEDULE DTSYNC

SPRING FALL CHANGE

SCHEDULE DTSYNC

SCHEDULE SOFTWARE MGMT

SCHEDULE BACKUP

Authorization Level 3: Test Access

TL1 Commands/Functions are NOT available for Authorization Level 3, Test Access (T) Functional Category.

Authorization Level 4: Maintenance

The **Functions available for Authorization Level 4, Maintenance (M) Functional Category** are the following:

ALL ALARM MONITORING

ENABLE FULL ALARM MONITORING

ENABLE PARTIAL ALARM MONITORING

PROVISION PROTECTION SWITCH

Authorization Level 4: Provision

The **Functions available for Authorization Level 4, Provision (P) Functional Category** are the following:

DCC TERMINATIONS

DCC PROVISIONING

ESTABLISH EQUIPMENT

IP TUNNELING

REMOVE EQUIPMENT

Authorization Level 4: Performance Mananagement

The **Functions available for Authorization Level 4, Performance Management (PM) Functional Category** are the following:

GLOBAL PM MGMT

NE PM MANAGEMENT

Authorization Level 4: Security

The **Functions available for Authorization Level 4, Security (S) Functional Category** are the following:

ADD AGGREGATE

ADD GNE ASSOCIATION

ADD NE

ADD SUBNET

ADD TRAIL

CHANGE AGGREGATE CONTENTS

DATE TIME MANAGEMENT

DELETE AGGREGATE

DELETE GNE ASSOCIATION

DELETE NE

DELETE SUBNET

DELETE TRAIL

GLOBAL PASSWORD ADMIN

MODIFY AGGREGATE

MODIFY GNE RNE ASSOCIATION

MODIFY NE

MODIFY SUBNET

NE SW ACTIVATE

NE SW COPY

NE SW DELETE

NE SW DOWNLOAD

NE SW TRANSFER

PROVISION DSA

RESTORE NE

RETRY INTERVALS

SCHEDULE SW ACTIVATE

SCHEDULE SW COPY

SCHEDULE SW DOWNLOAD

SWITCH ACTIVE GNE

VIEW DESCRIPTIVE INFORMATION

SUBNETWORK MANAGEMENT

ADD SUBNET

MODIFY SUBNET

DELETE SUBNET

UPDATE SYSTEM

SCHEDULE SW ACTIVATE

Authorization Level 4: Test Access

TL1 Commands/Functions are NOT available for Authorization Level 4, Test Access (T) Functional Category.

Authorization Level 5: Maintenance, Provision, Performance Management, and Test Access

TL1 Commands/Functions are NOT available for Authorization Level 5, Maintenance (M), Provision (P), Performance Management (PM), and Test Access (T) Functional Categories.

Authorization Level 5: Security

The **Functions available for Authorization Level 5, Security (S) Functional Category** are the following:

SCHEDULE SW COPY

SCHEDULE SW DOWNLOAD

RETRY INTERVALS

PROVISION DSA

DSA MANAGEMENTADD COMMAND GROUP

ADD TARGET GROUP

DELETE COMMAND GROUP

DELETE TARGET GROUP

MODIFY COMMAND GROUP

MODIFY TARGET GROUP

ADD USER

MODIFY USER

DELETE USER

DISPLAY LOGGEDIN USERS

GLOBAL SECURITY PROVISIONING

ADD NE USER

MODIFY NE USER

DELETE NE USER

RESET NE

PROCESSOR CONDITIONS

□

Index