Lucent Technologies
Bell Labs Innovations

Navis™ Optical Element Management System (EMS)

Administration Guide

Release 7.0

190-224-151R7.0
Issue 1.0
January 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 190-224-151R7.0.

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.

Lucent Technologies values your comments!

Lucent Technologies
Bell Labs Innovations

Navis ™ Optical Element Management System (EMS)
Administration Guide
Release 7.0
190-224-151R7.0 Issue 1.0 January 2002

Lucent Technologies welcomes your comments on this information product. Your opinion is of great value and helps us to improve.

1. Was the information product:

	Yes	*No*	*Not applicable*
In the language of your choice?	☐	☐	☐
In the desired media (paper, CD-ROM, etc.)?	☐	☐	☐
Available when you needed it?	☐	☐	☐

Please provide any additional comments:

_____

_____

2. Please rate the effectiveness of this information product:

	Excellent	*More than satisfactory*	*Satisfactory*	*Less than satisfactory*	*Unsatisfactory*	*Not applicable*
Ease of use	☐	☐	☐	☐	☐	☐
Level of detail	☐	☐	☐	☐	☐	☐
Readability and clarity	☐	☐	☐	☐	☐	☐
Organization	☐	☐	☐	☐	☐	☐
Completeness	☐	☐	☐	☐	☐	☐
Technical accuracy	☐	☐	☐	☐	☐	☐
Quality of translation	☐	☐	☐	☐	☐	☐
Appearance	☐	☐	☐	☐	☐	☐

If your response to any of the above questions is "*Less than satisfactory*" or "*Unsatisfactory,*" please explain your rating.

_____

_____

3. If you could change one thing about this information product, what would it be?

_____

_____

4. Please write any other comments about this information product:

_____

_____

Please complete the following if we may contact you for clarification or to address your concerns:

Name: _____ Date: _____

Company/organization: _____ Telephone number: _____

Address: _____

Email address: _____ Job function: _____

If you choose to complete this form online, go to http://www.lucent-info.com/comments
Otherwise fax to 407 767 2760 (U.S.) or +1 407 767 2760 (outside the U.S.) or email comments to ctiphotline@lucent.com

Lucent Technologies values your comments!

Lucent Technologies
Bell Labs Innovations

Navis ™ Optical Element Management System (EMS)
Administration Guide
Release 7.0
190-224-151R7.0 Issue 1.0 January 2002

Lucent Technologies welcomes your comments on this information product. Your opinion is of great value and helps us to improve.

1. Was the information product:

	Yes	*No*	*Not applicable*
In the language of your choice?	☐	☐	☐
In the desired media (paper, CD-ROM, etc.)?	☐	☐	☐
Available when you needed it?	☐	☐	☐

Please provide any additional comments:

_____

_____

2. Please rate the effectiveness of this information product:

	Excellent	*More than satisfactory*	*Satisfactory*	*Less than satisfactory*	*Unsatisfactory*	*Not applicable*
Ease of use	☐	☐	☐	☐	☐	☐
Level of detail	☐	☐	☐	☐	☐	☐
Readability and clarity	☐	☐	☐	☐	☐	☐
Organization	☐	☐	☐	☐	☐	☐
Completeness	☐	☐	☐	☐	☐	☐
Technical accuracy	☐	☐	☐	☐	☐	☐
Quality of translation	☐	☐	☐	☐	☐	☐
Appearance	☐	☐	☐	☐	☐	☐

If your response to any of the above questions is "*Less than satisfactory*" or "*Unsatisfactory,*" please explain your rating.

_____

_____

3. If you could change one thing about this information product, what would it be?

_____

_____

4. Please write any other comments about this information product:

_____

_____

Please complete the following if we may contact you for clarification or to address your concerns:

Name: _____ Date: _____

Company/organization: _____ Telephone number: _____

Address: _____

Email address: _____ Job function: _____

If you choose to complete this form online, go to http://www.lucent-info.com/comments
Otherwise fax to 407 767 2760 (U.S.) or +1 407 767 2760 (outside the U.S.) or email comments to ctiphotline@lucent.com

Contents

2 Security Management

List of Figures

List of Tables

About this information product

Purpose

This chapter is a preface that 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 7.0. The document has been reissued to describe new features for Navis™ Optical EMSRelease 7.0.

Safety labels

N/A

Intended audience

The purpose of this guide is to instruct users how to administer Navis™ Optical EMS. This guide is written primarily for operations personnel who will be administering 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	Describes this document's purpose and intended audience, how to use the document, and how to comment on it
Chapter 1	Chapter 1, "System Introduction"	Provides an general introduction to Navis™ Optical EMS and its functions/features
Chapter 2	Chapter 2, "Security Management"	Describes tasks performed to control access to Navis™ Optical EMS and its managed network elements
Chapter 3	Chapter 3, "System Administration"	Describes tasks performed to start up, shut down, and reboot the Navis™ Optical EMS application.
Chapter 4	Chapter 4, "Database Maintenance"	Describes tasks performed to maintain the Navis™ Optical EMS database.
Chapter 5	Chapter 5, "Management Communication of Navis™ Optical EMS"	Describes tasks performed to configure communication interfaces with network elements managed by Navis™ Optical EMS
Chapter 6	Chapter 6, "Trouble Clearing"	Describes tasks performed to facilitiate troubleshooting problems with software components of Navis™ Optical EMS and its communications interfaces
Chapter 7	Chapter 7, "Cluster Administration GUI Operations"	Describes task performed using the cluster administration GUI, which is a separate Navis™ Optical EMSGUI used to monitor redundant server operations.

Section	Title	Description
Chapter 8	Chapter 8, "Security Management Concepts"	Provides general information about controlling access to Navis™ Optical EMSand its managed network element
Chapter 9	Chapter 9, "Cluster Administration GUI for Geographically Redundant Navis™ Optical EMS Servers"	Provides general information about the cluster administration GUI, which is a separate Navis™ Optical EMSGUI used to monitor redundant server operations.
Chapter 10	Chapter 10, "Trouble Clearing Concepts"	Provides reference information to support tools used for troubleshooting Navis™ Optical EMS problems

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 above (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

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

Customer comment form

A customer comment form appears immediately after the title page of this document. Please fill out the form and fax it to the number provided on the form.

How to order

To order Navis™ Optical EMS information products:

Contact your Lucent Technologies customer team representative

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 System Introduction

Overview

Purpose

This chapter provides a general system overview of Navis™ Optical EMS.

Objectives

This chapter explains how to do the following:

- List the features available on the Navis™ Optical EMS and briefly describe each feature
- Identify the basic hardware components of Navis™ Optical EMS
- Identify the basic software components of the Navis™ Optical EMS
- Identify the network element types and releases supported by the Navis™ Optical EMS
- Identify the system interfaces of the Navis™ Optical EMS

Contents

System Overview

Description

The Lucent Technologies' *Navis*™ Optical Element Management System (EMS) supports the new generation of Lucent Technologies' transmission products: the Lucent Technologies' WaveStar® product family. The WaveStar® products are intelligent Network Elements (NEs) which can discover and report their configuration (including physical equipage) and connectivity within the network.

The Navis™ Optical EMS operates as an enhanced graphical tool and as a general configuration management aid. It is designed to take advantage of the capabilities of the WaveStar® NEs, and to optimize the role of the NEs in management functions to create an intelligent operations environment.

Just as the WaveStar® network elements are the solution to your transport network needs, the Navis™ Optical EMS is the answer to the corresponding operations needs to efficiently manage the network. The following details some of the ways that the Navis™ Optical EMSachieves this:

- Navis™ Optical EMS provides centralized, secure, remote administration of Synchronous Optical Networks (SONET) and Dense Wavelength Division Multiplexing (DWDM) subnetworks. From a single work center, a Navis™ Optical EMS user can remotely manage SONET and DWDM NEs. Lucent Technologies patented Dynamic Network Operations (DNO) process gathers network configuration information from the NEs, providing accurate, hands-off population of the Navis™ Optical EMSdatabase, and ensures that the Navis™ Optical EMS management functions operate using the actual network configuration.
- Navis™ Optical EMS provides fault, performance, configuration, security, and log management functions via the GUI.
- Navis™ Optical EMS supports 7-layer OSI as well as OSI over Transmission Control Protocol/Internet Protocol (TCP/IP) communication protocols over LAN physical interfaces.
- Navis™ Optical EMS supports X.25-based protocol layer for Lucent Technologies' FT-2000 Large Capacity Terminal (LCT).
- Navis™ Optical EMS supports CMISE and TL1 application protocols.

- Navis™ Optical EMS supports communication multiplexing or concentration to provide network security and to record all database changes.
- Navis™ Optical EMS provides a TL1 cut-through capability, allowing the user to access an NE through a native command set.

Graphical user interface

Navis™ Optical EMS incorporates a platform independent, Java-based Graphical User Interface (GUI) that allows for the use of PCs running Windows NT as the user's terminals. The Navis™ Optical EMS GUI is a common interface to all NEs, regardless of type, and provides a powerful, flexible, and user friendly interface to execute the most frequently used actions. The GUI also supports numerous customization options so that users may tailor the displays in accordance with their own preferences.

The GUI 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 provides the ability to initiate a cut-through session to directly send TL1 commands to NEs.

Year 2000 compliance

Navis™ Optical EMS and the underlying software platforms are designed to comply with the Year-2000 initiative to ensure correct date representation and date/time calculation for the year 2000 and beyond. Navis™ Optical EMS Release 4.2 and UNIX Release 11.0 are Year-2000 compliant only when the required Year-2000 patch set (Y2K-1020S800) is installed. This includes data that is received by the Navis™ Optical EMS from the supported NEs.

□

Features

Overview

Navis™ Optical EMS provides a set of standard and value-added features used to administer the WaveStar® NEs. These are grouped into the following categories:

- Fault Management
- Performance Management
- Configuration Management
- Security Management
- Log Management
- NE Event Handler
- Cut-Through Capability

Fault management

Fault Management monitors alarms and conditions in the subnetwork. Navis™ Optical EMS receives autonomous alarm messages from NEs when alarm states are set or cleared. These alarm messages are processed and made available to the user through the GUI, or to other network surveillance systems. Navis™ Optical EMS supports the following Fault Management tasks:

- Alarm status indication on the network map for equipment, facility failures, and updates
- Hierarchical alarm status indication at NE, bay, shelf, and circuit pack levels
- Textual alarm summary report
- Alarm provisioning at the NE level (via TL1 cut-through)
- Alarm provisioning at the EMS level
- Alarm synchronization
- Autonomous alarm handling
- Alarm correlation
- Alarm aging

Performance management

Navis™ Optical EMS collects Performance Monitoring (PM) data from NEs that have PM data collection activated. It stores collected PM data for a retention period set by the user (up to 30 days). Navis™ Optical EMS allows the user to view unprocessed PM data, or the data can be exported to an off-line system for more sophisticated analysis and reporting purposes.

Configuration management

Navis™ Optical EMS has a Dynamic Network Operations (DNO) feature that retrieves the internal configurations of NEs and external connectivity relationships. This feature enables the system to discover, without manual intervention, the topology of subnetworks consisting of Lucent Technologies' NEs.

The GUI supports the following configuration management tasks:

Subnetwork configuration management

- Network Element/trail discovery/update/display
- Aggregate management/display

NE configuration management

- Equipage discovery/update/display
- Equipment provisioning and pre-provisioning
- Cross-connection provisioning/display
- Tributary reservation
- Manual path provisioning
- Protection switch management
- Port provisioning

Software management

- Software download to NEs
- Software copy from one NE to another
- Software install (activate) on NE
- NE data backup and restore

Security management

Navis™ Optical EMS maintains a set of connections to the NEs that are shared by all users. Administration of individual user logins and passwords is centralized on Navis™ Optical EMS rather than distributed across the large number of managed NEs.

All users are required to have a login and password to communicate with the system. The system administrator assigns users to the NEs

they can use (Target Groups) and the actions they can perform (Command Groups). Target Groups and Command Groups can be set up according to the type of tasks users are performing, such as maintenance, provisioning, or monitoring.

Navis™ Optical EMS provides two levels of security management:

- EMS security management
  - defines EMS users (user id and password)
  - partitions the network into user-defined target groups
  - defines command groups
  - assigns EMS user to target groups and command groups
- NE security management
  - provides services to manage NE user id and password

Log management

Log Management provides services to various system modules including:

- Writing log messages to database tables
- Retrieving log messages from database tables
- Displaying information on selected activities

These log messages are helpful for keeping track of information regarding system performance and actions. The information can be filtered to suit the user's needs.

NE event handler

The NE Event Handler process is a passive distributor of non-alarm autonomous messages emitted by the NEs. It registers with the Southbound interface for database change messages from TL1 NEs and with Q3 gateway for CMISE NEs.

The main functions of the NE Event Handler (NEH) are the following:

- Receive non-alarm autonomous messages (TL1 from Southbound and CMISE from Q3 gateway)
- Distribute the received messages to the user
- Log by invoking the Log Manager

Cut-through capability

In order for the user to execute NE TL1 commands that may not be explicitly supported, a cut-through capability is available. Navis™ Optical EMS allows the user access only to the NEs and associated commands defined by the Target and Command Groups for which the user is assigned.

□

Hardware Architecture

Overview

Navis™ Optical EMS consists of a Hewlett-Packard (HP) host processor, and GUI workstations (PC/Sun) connected via an Ethernet LAN, with the option to interface via a Wide Area Network (WAN).

A WAN/PSN is recommended for large, geographically dispersed configurations to concentrate access from the Navis™ Optical EMS to the managed subnetworks. The same WAN/PSN can also be used to access other network management systems or other hosts. Every Navis™ Optical EMS installation requires data connections to each managed subnetwork.The southbound WAN from the Navis™ Optical EMS to the NEs must support an OSI/LAN interface and/or an IP/LAN interface. If FT-2000 LCT NEs are to be managed, an X.25 PSN is required.

Host platform

The system hardware architecture consists of two main components:

- HP K-class, L-class, or N-class server running HP-UX version 11.0 (Nov. 1999) with associated peripherals (console, terminals, and printers)
- PC running *Windows NT*® 4.0 (ServicePack 4) or Windows 2000
- Sun Solaris workstation Version 2.6 or 2.7.

GUI workstation

The recommended platform for the Java GUI client is a personal computer running Windows NT 4.0 with ServicePack 4 or Windows 2000. The Java GUI software is installed on the PC as a standalone application. Transaction requests are issued by the GUI software to the EMS host. The host returns responses associated with these transactions back to the PC. The interface to the PC is via an 802.3 LAN link. The GUI application messages and GUI cut-through data traffic are transported using this interface.

System redundancy options

The Navis™ Optical EMS system redundancy option provides multiple levels of application and host redundancy for backup support and disaster recovery in the event of failure. The local and geographic redundancy configurations require two similarly equipped hosts that operate in an active/standby arrangement. The two host computers are linked via a TCP/IP WAN segment and employ data replication to provide near real-time database synchronization of the standby host with the currently active host.

Under normal operating conditions, the Navis™ Optical EMS application is running on the active host, with that host actively monitoring all network elements in the management domain. The backup host is in a hot-standby state, maintaining data connections to the network, and using data replication from the active host to keep its database current. In the event of a primary host failure, an administrator can switch manually to the standby host or a switchover can be set up to be performed automatically through the cluster adminstration GUI. Upon switch-over, the standby host assumes active control of the network.

For details about the cluster administration GUI, refer to the *Navis™ Optical EMS Administration Guide.*

The Navis™ Optical EMS redundancy options include:

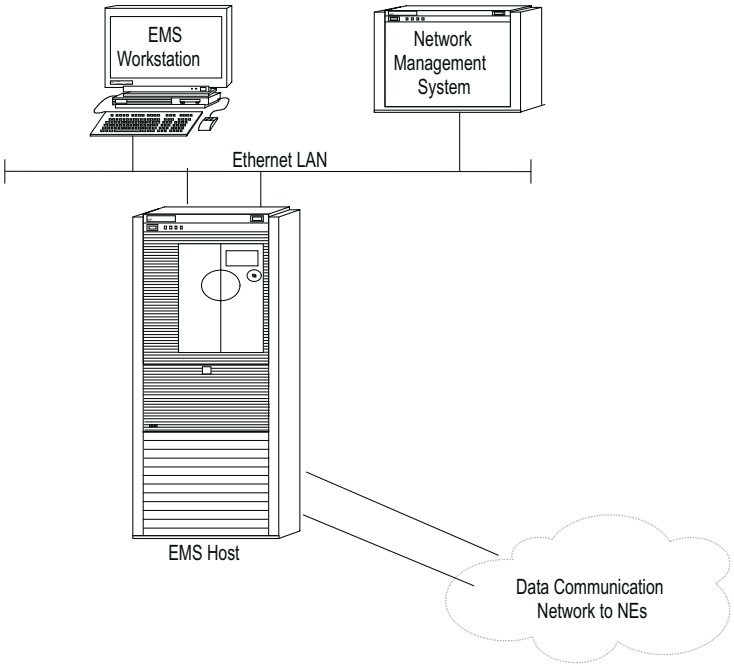
- host redundancy
- local redundancy
- geographic redundancy

Host redundancy

Host redundancy provides component redundancy within a single host where there is no backup host available (Figure 1-1, “EMS Basic Host Standalone Configuration” (1-10)). Recovery relies on switching

control to another resource on the same host such as a backup LAN card or mirrored disk.

Figure 1-1 EMS Basic Host Standalone Configuration

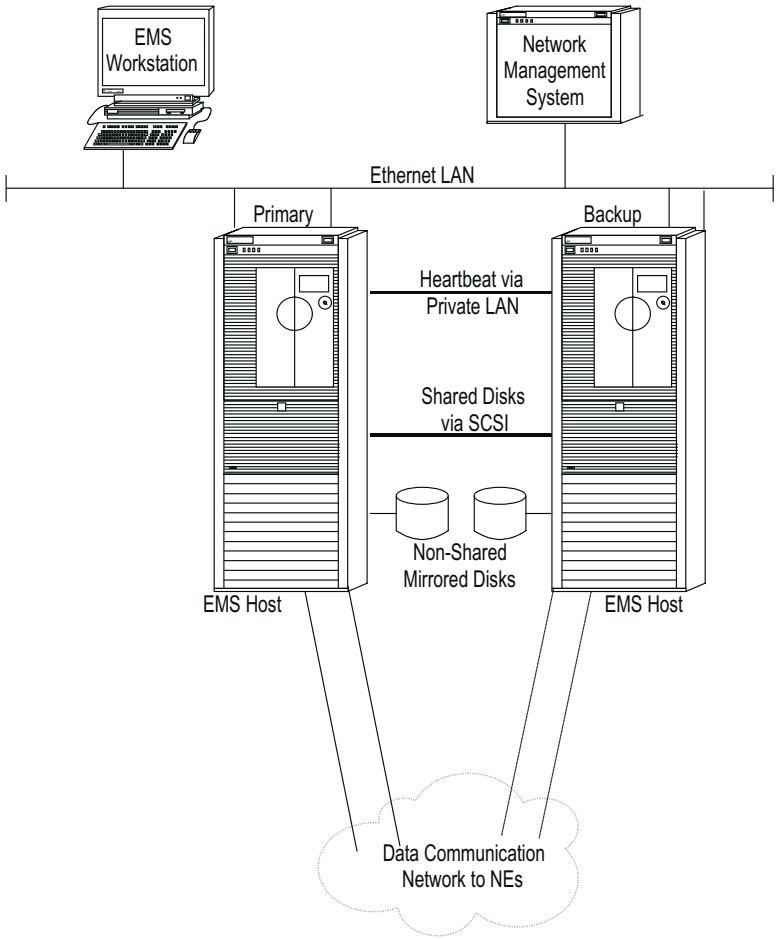


Local redundancy

Local redundancy employs two similarly equipped hosts located in the same building (Figure 1-2, “EMS Local Redundancy Configuration” (1-11)). Each host is configured with redundant hardware components.

Should the primary host fail, the backup host is activated automatically without user intervention.

Figure 1-2 EMS Local Redundancy Configuration



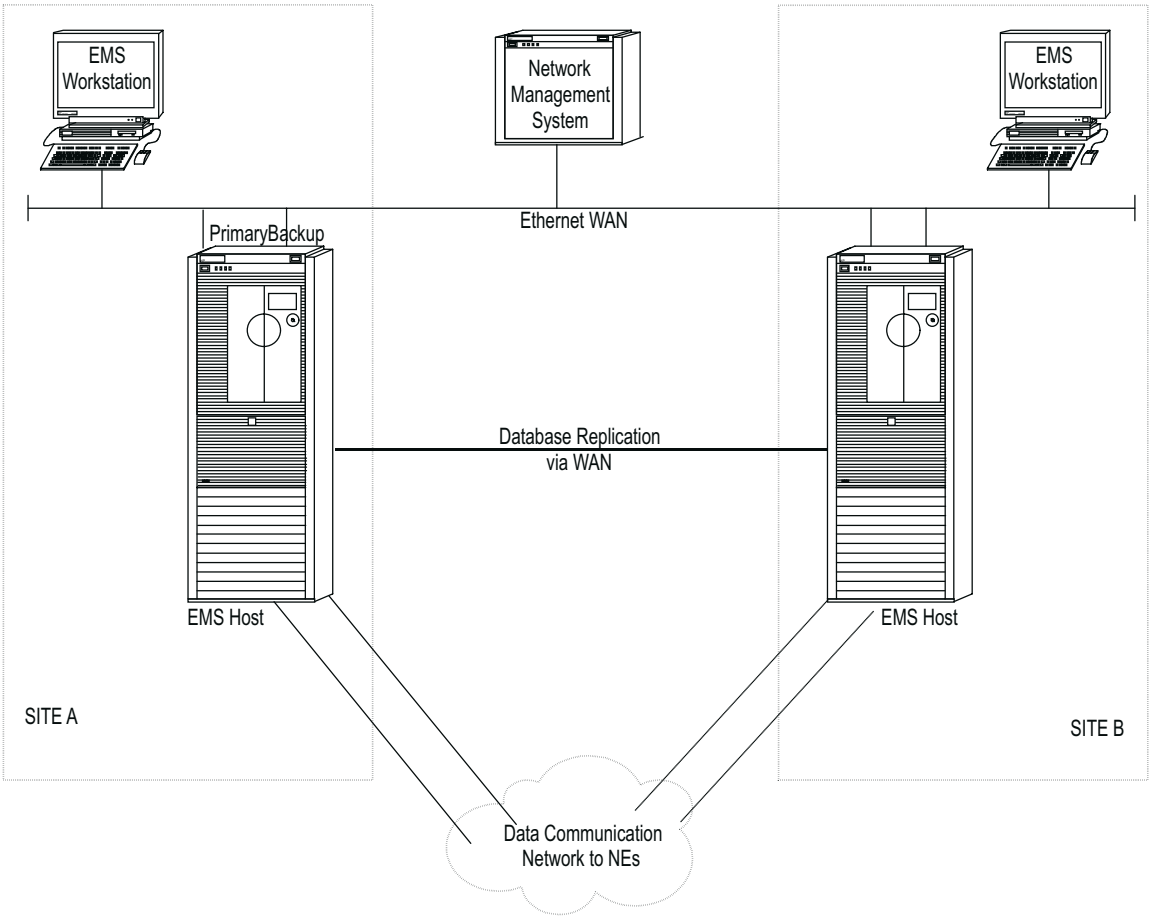
Under normal operating conditions, the Navis™ Optical EMS Host is in service (or “active”) on the primary host monitoring all network elements in the database. The backup host exists in a passive (or “standby”) mode. This configuration uses a “floating” IP address shared by both servers. Although the “standby” host is logged into all network elements, it does not initiate any event to the network or react to any notifications from the network. Database synchronization is handled using Informix Enterprise Replication, FTP file transfer, and event forwarding from the “active” host. In the event of a primary host failure, control is automatically switched from the primary to the backup host, changing the Navis™ Optical EMS application from

"standby" to "active" service without user intervention. Once the primary host failure is repaired, it can be quickly and easily configured to act as the new standby host with no interruption in service.

Geographic redundancy

Geographic redundancy employs two similarly equipped hosts located in different geographical locations (like Atlanta, GA, and Denver, CO (Figure 1-3, "EMS Geographic Redundancy Configuration" (1-12)). Each host is configured with redundant hardware components, and resides on a TCP/IP WAN segment. Data replication and event forwarding via ***ftp*** over a WAN are used to maintain EMS database and UNIX file system synchronization.

Figure 1-3 EMS Geographic Redundancy Configuration



Under normal operating conditions, the Navis™ Optical EMS application is in service (or “active”) on the primary host monitoring all network elements in the database. The backup host exists in a passive (or “standby”) mode with the Navis™ Optical EMS application running in a “read only” mode. Although the “standby” host is logged into all networks, it does not initiate any event to the network or react to any notification from the network. Database synchronization is handled using Informix Enterprise Replication, FTP file transfer, and event forwarding from the “active” host. In the event of a primary host failure, control can be manually or automatically switched from the primary to the backup host changing the Navis™ Optical EMS application from “standby” to “active” service.

In a geographic redundant server configuration, switchover from the primary to the backup server can be performed either manually or by using the automatic switchover feature which can be set up through the cluster Administration GUI. Once the primary host failure is repaired, it can be quickly and easily configured to act as the new standby host with no interruption in service.

For details about the cluster administration GUI, refer to the *Navis™ Optical EMS Administration Guide.*

□

Software Architecture

Overview

The software architecture can be divided into the following major subsystems:

- Configuration Management
- Fault Management
- NE Event Handler
- EMS Security Management
- Southbound Management Interface
  - X.25-based protocol layer
  - OSI-based protocol layer
  - OSI over TCP/IP-based protocol layer
  - TL1 Manager
  - Connection Manager
  - Gateway process
  - QA process (CMISE only)
  - SONET Directory Service (SDS)
- Log Management
- Operation, Administration, and Maintenance
  - Log and trace
  - Scheduler
- JAVA-based GUI

□

Supported Network Elements

Overview

Navis™ Optical EMS provides element management support for the following NEs and their software releases. The information is the best available at the time of publication of this document and is subject to change based on the availability of the NE releases.

Table 1-1 Network Elements Supported by Navis™ Optical EMS

Managed NEs	Supported Releases
WaveStar® Bandwidth Manager (BWM)	R1.2, R1.3, R2.0, R3.0, R3.1, R4.0, R4.1
WaveStar ®OLS 1.6T	R2.0, R3.0, R4.0, R5.0, R6.0, R6.1
WaveStar®Network Communications Controller (NCC)	R3.0, R3.1, R3.2
WaveStar TDM 2.5G (OC-48 2F)/WaveStar® TDM 10G(OC-192 2F)	R2.0, R3.0, R4.0, R5.0 (10G shelf option available beginning in R3.0), R5.0.2, R5.1.2, R5.1.5, R6.1.5
WaveStar TDM 10G (OC-192 2F)	R1.0, R1.1, R2.0, R2.1
WaveStar*WaveStar*TDM 10G (STM-64)	R1.0, R1.1, R2.0, R2.1, R2.2, R3.0, R4.0.5
FT-2000 LCT	R4.0
LambdaRouter™All Optical Switch (AOS)	R2.0
Metropolis™ DMX Access Multiplexer	R1.1, R2.0
Metropolis Enhanced Optical Networking (EON)	R7.0, R7.5, R8.0, R8.1
Metropolis DMX***press***Access Multiplexer	R1.0
LambdaUnite™ MultiService Switch (MSS)	R2.0

System Interfaces

Overview

The Navis™ Optical EMS southbound communication interface connects with NEs, and supports OSI and OSI over TCP/IP communications with the NEs.

- WaveStar™ OLS 1.6T supports both an OSI and OSI over TCP/IP interface.
- WaveStar® BWM and WaveStar® TDM 2.5G only support an OSI interface. However, since the NCC acts as a transport bridge, the Navis™ Optical EMS also supports an OSI over TCP/IP interface to WaveStar® BWM and WaveStar® TDM 2.5G NEs via a transport bridge.
- WaveStar® NCCs support both OSI and OSI over TCP/IP interfaces, much like the WaveStar™ OLS 1.6T.

Configuration management

The Configuration Management subsystem (CF) provides the following functions for the Navis™ Optical EMS:

- discovers the network and its elements that are in an EMS domain
- maintains an information model of the network and its elements concerning configuration management
- provides the cross connection service
- provides protection switching management service
- derives the provisionable subnetworks
- provides the path provisioning services on these subnetworks
- provides NE parameter provisioning
- provides NE Synchronization Management

The Configuration Management Functional Area (MFA) CF is designed as an Navis™ Optical EMS network configuration management server. It provides services to accomplish configuration management tasks. Configuration Management, in turn, uses the services of other Navis™ Optical EMS subsystems to handle user requests.

Fault management

The Fault Management subsystem (FM) serves the following functions for Navis™ Optical EMS:

- Alarm collection and storage
- Alarm processing: (Aging, Event Per Time, Alarm correlation and suppression)
- Alarm broadcast
- Alarm severity assignment profile management
- Alarm database synchronization
- Alarm log synchronization

FM does not have any direct interface to external systems. FM has interfaces to a number of other Navis™ Optical EMS application subsystems.

NE event handler

The main functions of the NE Event Handler (NEH) are:

- receiving non-alarm autonomous messages
- distributing the messages received to clients.
- Logging messages by invoking the Log manager.
- Performing Security Log resynchronization upon re-establishment of an NE communications link.

The NE Event Handler process is a passive distributor of non-alarm autonomous messages emitted by the NEs. It receives non-alarm autonomous messages regarding TL1 NEs from the southbound TL1 processes (CS_Southbound and CS_SbOsi), and receives notifications regarding CMISE NEs from southbound Q3 gateway. The messages received from southbound TL1 processes are TL1 message strings as received from the NE while the CMISE notifications are in MFA structures.

Southbound interface

The Navis™ Optical EMS Southbound interface contains the required functionality to connect to the NEs, to manage these connections, and to forward and receive the messages between the NEs and Navis™ Optical EMS, for all supported communication protocols.

Connection Manager Process

The Connection Manager (CM) process centralizes the functions of sending, receiving, routing, and processing the connections needed for responses and autonomous messages going in, and coming from, the

CMISE and TL1 Southbound subsystems. CM handles the following functions:

- At start-up, load external configurative parameters from a configuration file.
- Create and terminate associations to all NEs.
- Perform association requests in a staggered manner to minimize the impact of the connection processes on the network.
- Implement association recovery mechanisms.
- Receive connection-related indication messages from TL1 and CMISE Southbound subsystems, update association status in memory, and forward notifications to Navis™ Optical EMS.
- Create/modify/delete NEs, store and forward related information.
- Send notification to Navis™ Optical EMS for any incorrect NE types.

CMISE Southbound

The CMISE Southbound subsystem is made of two processes for the support of Lucent Technologies' WaveStar™ OLS 1.6T NEs.

- Gateway (GW) process
  - serves as a bridge process between the Management Functional Area (MFA) and the Q3 Manager
  - receives requests from MFA and the Connection Manager, and sends them down to the Q3 Manager through a socket interface
  - receives responses and autonomous notifications coming from NE via socket. Sends them to MFA or the Connection Manager as required.
  - logs Command and Responses, via the Log Server and Log library.
- Q3 Adaptor process
  The Q-Adaptor maintains a representation of the manged object instances of the managed object classes defined in the information model and converts Common Management Information Service Element (CMISE) requests into the non-TMN format of the underlying OS or NE. It also converts the non-TMN notifications received from a non-TMN OS or NE and converts them to CMISE notifications.

TL1 Southbound

TL1 Southbound is supported by the TL1-Manager process, which is responsible for command/response handling.

SONET Directory Services

The SONET Directory Services (SDS) subsystem resides in the Southbound of the system. All system applications access the shared memory contained in SDS to retrieve information. The shared memory contains the status, last update time, and various directory information. Navis™ Optical EMS employs two agents to manage this information: the Directory Services Agent (DSA) and the Directory User Agent (DUA). The DSA maintains the Directory Information Base and the DUA retrieves and gives information to and from it.

The DSA organizes network elements into a structure known as the Directory Information Base (DIB). The DUA accesses the DSA for any new NEs registered in the MIT and notifies other Navis™ Optical EMS processes of the existence of the new NE. Navis™ Optical EMS then logs into the new NE and via the Dynamic Network Operations (DNO) process gathers the internal configuration and external connectivity relationships from the NE. This ensures that the Navis™ Optical EMS management functions operate using the actual network configuration.

Northbound interface to Navis™ Optical NMS

Navis™ Optical EMS supports a northbound interface to the Navis ™ Network Management System (Navis™ Optical NMS). Navis™ Optical NMS is a part of a telecommunications management network that provides comprehensive and integrated management of an entire transport network. Navis™ Optical NMS manages network elements through an interface with Navis™ Optical NMS. The Navis™ Optical EMSexchanges NE alarm information, configuration information, and performance monitoring data with Navis™ Optical NMS, through a standard CORBA interface.

There are two Navis™ Optical NMS interfaces supported by the Navis™ Optical EMS. The first interface is a server to server interface and the other interface is a GUI to GUI interface.

The server to server interface is responsible for passing NE information from the Navis™ Optical EMS to the Navis™ Optical NMS. The northbound interface to the Navis™ Optical NMS is called the Telecommunications Management Forum (TMF) CORBA Northbound Interface.

The GUI to GUI cut-through allows the Navis™ Optical NMS to invoke the Navis™ Optical EMS GUI screens from the Navis™ Optical NMS GUI. This feature is called the F-interface in both the Navis™ Optical NMS and the Navis™ Optical EMS terminology. Both GUIs must be installed on an NT Terminal Server and be properly configured to talk to one another. The interface supports a one-to-many configuration where one Navis™ Optical NMS GUI can talk to many Navis™ Optical EMS GUIs of different versions.

□

2 Security Management

Overview

Purpose

This chapter describes procedures performed to control access to Navis™ Optical EMS and its managed network elements.

Before you begin

Read Chapter 8, "Security Management Concepts" to acquire a basic understanding of the Security Management features provided by Navis™ Optical EMS.

Contents

Change Your User Password

Purpose

Use this procedure to change your user password.

Valid password

A valid password is 6-10 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 (3) characters. For comparison purposes, an uppercase letter and its corresponding lowercase equivalent are treated as identical. This means, the new password must contain at least three (3) new and different characters that were not present in the old password. For example: It is valid to change the password “ems+123” to “abc+123” because all three characters ‘a’, ‘b’ and ‘c’ were not present in the old password. It is not valid to change the password “ems+123” to “ems+321” because no “new” characters have been introduced in the new password.

The new password cannot contain the user (login) ID as part of the password; for example, a login ID “john” cannot have a password of “john+123”.

Use of previous passwords

The Global Security Provisioning feature in Navis™ Optical EMSallows the Navis™ Optical EMS 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 recalled and prevented from re-use by Navis™ Optical EMS is five passwords. This parameter can be disabled by the administrator by setting the value to zero (0) so that the system does not recall any previous passwords.

Related tasks

Refer to the following related tasks:

- “Modify a User” (2-13)
- “Globally Provision User Login/Password Parameters (Global Security Provisioning Feature)” (2-49)

Task Complete the following steps to change your user password.

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

Result:

This displays a sub-menu.

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

Result:

This displays another sub-menu.

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 desired new password into the New Password field.

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

7

IF...	THEN...
the new password entered is invalid	the system issues a warning message. You must enter a password that is 6-10 characters, contains at least two alphabetic characters, at least one numeric character, and one special character (!#$%^&*()-+_=?). The following special characters are not permitted (:,;). A password cannot contain the user ID as a sub-string; for example, a user ID “john” cannot have a password of “john+123”, “johnny+1”, or “iamjohn+1”.

IF...	THEN...
you change the password to one previously used	If the “previous password” option in the Global Security Provisioning window is enabled, the system issues a message, advising that you cannot change the password to one previously used and that a different password must be chosen.

8 Select the OK button 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

Before you begin this task, you must be logged into Navis™ Optical EMS. The NE(s) or aggregate(s) for which you are changing passwords must already exist in Navis™ Optical EMS. Be aware that if you are changing passwords for 20 or more NEs at a time, this may degrade system performance. Only one user can use the Global Administer NE Password function at a time.

Be aware that any changes to the primary/secondary passwords for NEs will affect logging into the NEs from all EMS and CIT interfaces.

BWM and TDM 10G (STM-64) NEs have a password aging feature for security reasons. When a software upgrade is performed for one of these NE types, 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 by the CIT. These default NE passwords are used by Navis™ Optical EMS to log into the NE and obtain information during the subnetwork autodiscovery process. The default NE passwords changed by the CIT during the software upgrade may not be known by Navis™ Optical EMS. However, as long as the second default NE password remains the same, Navis™ Optical EMS will be able to use it to log into the NE during subnetwork autodiscovery.

Once Navis™ Optical EMS has been able to log into a Navis™ Optical EMS BWM or WaveStar® TDM 10G NE using the unchanged default NE password, you should use the Global Password Administration feature described in this task to manually change the NE password of the Super User Login that was changed by the CIT during installation. Then, Navis™ Optical EMS has access to both Super User NE logins/passwords to log into WaveStar® BWM and WaveStar® TDM 10G NEs.

If one or both passwords that 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 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. Refer to the NE hardware documenation for the TL1 command needed to turn off the password aging feature.

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. Before using this feature, make sure that you really want to proceed with changing the primary/secondary passwords.

To perform this task, access the Map window.

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

1 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.

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 Password Administration** from the Security sub-menu.

Result:

The Global Password Administration window is displayed.

5

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.

6 Select the NE(s) or aggregate(s) for which the password(s) will be changed, from the Network Elements/Aggregates list. When you select an NE or aggregate, the item moves from the Network Elements/Aggregates List to the Chosen NEs list.

You can use the arrow push buttons to move NEs/aggregates back and forth between the two lists, as needed.

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

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

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

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

11 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.

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

Important! 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. 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. A unique user ID (login) must be defined for each user that accesses Navis™ Optical EMS.

When adding a user ID, you also define the NEs that can be accessed using this login and the commands that can be issued to those accessible NEs. For each user ID, you 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 ID.

Related information

For additional information, see the following:

- Chapter 8, "Security Management Concepts"
- "Add a Target Group" (2-23)
- "Add a Command Group" (2-17)

Task

Complete the following steps to add a user login.

1 Select **Administration** from the main menu bar on the Map window. 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 2-10 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 1-20 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 6-10 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 Network Management System (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 a user login's attributes. The Login Type, Alias, Password, Command Group, and/or Target Group can be changed.

Before you begin

Before you begin this task, you must create a user login.

To perform this task, access the Map window.

Valid user ID

A valid User ID (login) is 3-10 alphanumeric characters in any combination. Special characters (such as ;*&@) are not allowed.

Valid password

A valid password is 6-10 characters. A user password can be 6-10 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 (:,;).

A new password cannot contain the user ID as a sub-string. For example, a user ID of "john" cannot have a password of "john+123", "johnny+1", or "iamjohn+1".

A new password must differ from the old one by at least three (3) characters. For comparison purposes, an uppercase letter and its corresponding lowercase equivalent are treated as identical. This means, the new password must contain at least three (3) new and different characters that were not present in the old password. For example: It is valid to change the password "ems+123" to "abc+123" because all three characters 'a', 'b' and 'c' were not present in the old password. It is not valid to change the password "ems+123" to "ems+321" because no "new" characters have been introduced in the new password.

Modifying attributes of pre-defined user IDs

Modification of attributes of pre-defined user IDs is not permitted. Only the password of a a pre-defined user ID can be changed.

Use of previous passwords

The Global Security Provisioning feature in Navis™ Optical EMS allows the Navis™ Optical EMS 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 recalled and prevented from re-use by Navis™ Optical EMS is five passwords. This parameter can be disabled by the administrator by setting the value to zero (0) so that the system does not recall any previous passwords.

Related tasks

Refer to the following related tasks:

- "Change Your User Password" (2-3)
- "Globally Provision User Login/Password Parameters (Global Security Provisioning Feature)" (2-49)

Task

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

1 Select **Administration** from the main menu bar on the Map window. 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 Select a user login from the list.

5 Click the Modify button.

Result:

The Modify User window is displayed.

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

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

To perform this task, access the Map window.

Task Complete the following steps to delete a user.

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

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

5. Click the Delete button.

   Result:

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

6. Choose Yes to delete the user.

END OF STEPS

□

Add a Command Group

Background

Use this procedure to add a Command Group. A Command Group is a set of NE and Navis™ Optical EMS commands that a user can use. In creating a Command Group, you can copy a set of commands from an existing command group into the new one. Command Groups can also be modified or deleted.

When a new user ID is created, you select which Command Group can be accessed by the user.

A maximum of 100 Command Groups (pre-defined and user-defined) is allowed.

Related information

For additional information, see the following:

- Chapter 8, "Security Management Concepts"
- "Add a User" (2-10)
- "Add a Target Group" (2-23)

Task

Complete the following steps to add a Command Group.

1 Select **Administration** from the main menu bar on the Map window. 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. The Status window is displayed, indicating the Command Group is being added to Navis™ Optical EMS.

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 Before you begin this task, be aware that 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.

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 theNavis™ Optical EMS.

Before you begin Before you begin this task, be aware that users for the Command Group being deleted must be reassigned to another Command Group. The reassignment is done as part of this task.

To perform this task, you must first access the Map window.

Task Complete the following steps to delete 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 Adminstration 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 deleted from the list.

5 Click the Delete button.

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

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

8 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. 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 group. Navis™ Optical EMS is initially loaded with two Target Groups: one for all NEs and another with no NEs. Additional Target Groups can be defined as needed by a system administrator or a user with a privileged login. In creating a Target Group, you can copy a set of NEs from an existing Target Group into the new one. Target Groups can also be modified or deleted.

A maximum of 100 Target Groups (pre-defined and user-defined) is allowed.

The Target Group and Command Group that a user can access is defined when a new user ID is created.

Before you begin

Before you begin this task, access the Map window.

Related information

For additional information, see the following:

- Chapter 8, “Security Management Concepts”
- “Add a User” (2-10)
- “Add a Command Group” (2-17)

Task

Complete the following steps to add a Target 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 **Target Groups** from the Security sub-menu.

Result:

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

4 Click the Add button.

Result:

The Add a Target Group window is displayed.

5 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.

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

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

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 Before you begin this task, be aware that 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.

To perform this task, access the Map window.

Task Complete the following steps to modify a Target 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 **Target Groups** from the Security sub-menu.

Result:

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

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

5 Click the Modify button.

Result:

The Modify Target Group window is displayed.

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

7 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 Before you begin this task, be aware that 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.

To perform this task, access the Map window.

Task Complete the following steps to delete a Target 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 **Target Groups** from the Security sub-menu.

Result:

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

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

5 Click the Delete button.

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

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

8 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 Before you begin this task, the NE(s) to which you want to add the NE login must exist in Navis™ Optical EMS.

To perform this task, access the Map window.

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

1 Select an NE on the Map window.

For instructions on selecting an NE, see the sub-procedure "SE 2–1: Selecting NEs and Aggregates on the Map Pane" (2-32) immediately following this procedure.

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 Click the Add button.

Result:

The Add login window for the chosen NE is displayed.

6 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 6-10 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 arrrow 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.
- 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.

- 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.

7 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

□

SE 2–1: Selecting NEs and Aggregates on the Map Pane

Procedure

1 To select a single NE or aggregate on the Map pane, position the mouse pointer over the NE or aggregate icon and click the select mouse button.

END OF STEPS

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. 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. As items in the Map pane are selected, they change color. Release the mouse select button. The items are selected.

END OF STEPS

Procedure

1 To deselect a selected item in the Map pane, position the mouse pointer over the item and single-click the mouse select button. 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.

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.

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

1 Select an NE on the Map window.

For instructions on selecting an NE, see the sub-procedure "SE 2–1: Selecting NEs and Aggregates on the Map Pane" (2-32) immediately following this procedure.

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, 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

□

SE 2–2: Selecting NEs and Aggregates on the Map Pane

Procedure

1 To select a single NE or aggregate on the Map pane, position the mouse pointer over the NE or aggregate icon and click the select mouse button.

END OF STEPS

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. 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. As items in the Map pane are selected, they change color. Release the mouse select button. The items are selected.

END OF STEPS

Procedure

1 To deselect a selected item in the Map pane, position the mouse pointer over the item and single-click the mouse select button. 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.

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 Before you begin this task, be aware than you cannot delete an NE login with a Super-Use 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.

For instructions on selecting an NE, see the sub-procedure "SE 2–1: Selecting NEs and Aggregates on the Map Pane" (2-32) immediately following this procedure.

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 Choose Yes to delete the NE login.

END OF STEPS

□

SE 2–3: Selecting NEs and Aggregates on the Map Pane

Procedure

1 To select a single NE or aggregate on the Map pane, position the mouse pointer over the NE or aggregate icon and click the select mouse button.

END OF STEPS

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. 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. As items in the Map pane are selected, they change color. Release the mouse select button. The items are selected.

END OF STEPS

Procedure

1 To deselect a selected item in the Map pane, position the mouse pointer over the itme and single-click the mouse select button. 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.

END OF STEPS

□

Terminate 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 Before you begin this task, see if the user is currently on the system via the Display Users window.

To perform this task, access the Map window.

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

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

Result:

The Terminate EMS User Sessions window is displayed.

4 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 the arrow push buttons to move user logins back and forth between the two lists, as needed.

5 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.

6 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 Before you begin this task, be aware that the `ems` login and other pre-defined logins may not be disabled. To see if a user is currently on the system, access the Display Users window through the GUI.

To perform this task, access the Map window.

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

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

Result:

The Disable/Enable User Sessions window is displayed.

4

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.

TO...	SELECT...
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!** You can use the arrow push buttons to move users back and forth between the two lists, as needed.

5 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

□

Display Logged In Users

Purpose Use this procedure to display all users that are currently logged into the Navis™ Optical EMS.

Before you begin Before you begin this task, access the Map window.

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

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 **Display Logged-In 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.

4 Click the Close button to close the window.

END OF STEPS

□

List Active Users on NE

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

Before you begin Before you begin this task, access the Map window.

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

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 **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.

4

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

5 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.

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

Result:

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.

7 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.

8 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.

9 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 there are no alarms 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(ies) are printed to the selected printer destination. If there are no alarms on the Alarm List, a message is displayed.

10 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

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

To perform this task, access the Map window.

Task

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

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

Result:

The Global Security Provisioning window is displayed.

4 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 thse 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 there are no multiple sessions active for that login type, then no warning message is 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.

5 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 which offers a greater security via more stringent password and authentication policies.

Before you begin

Conversion to a trusted system should take place only 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 Fore related information, refer to "Convert to Trusted Mode System" (2-52)

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

□

3 System Administration

Overview

Purpose

This chapter describes the procedures for stopping, restarting, and rebooting a simplex (non-redundant) Navis™ Optical EMS system, and reinstalling the HP OpenView License.

Contents

Bring Down the Navis™ Optical EMS Application (Non-Redundant System)

The Navis™ Optical EMS application runs continuously on the host computer under normal operating conditions, gathering and routing network information. The procedures in this section describe how to start and stop the execution of the Navis™ Optical EMS application on a simplex (non-redundant) host computer should this become necessary.

- The host computer needs to be rebooted
- The Navis™ Optical EMS database needs to be restored
- A power outage affects the host computer
- A Navis™ Optical EMS problem needs to be corrected

Important! Ordinarily the Navis™ Optical EMS application is stopped only under the following conditions:

Task Perform the following steps to bring down the Navis™ Optical EMSapplication.

1 Log into the Navis™ Optical EMS host computer using the `ems` login.

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

3 After the application has been brough down, confirm that the application is in shutdown mode by typing `appstat` and then pressing the Return/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 (Non-Redundant System)

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

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

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

3 When your screen displays a prompt asking whether to delete trace files, respond with `y` and press the Return/Enter key, unless the trace files are needed to diagnose a system problem.

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

Result:

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

END OF STEPS

□

Reboot the Navis™ Optical EMS Application (Using Shutdown Command) (Non-Redundant System)

Purpose The Shutdown Command can be used to reboot the Navis™ Optical EMS application. This command will gracefully shut down the Navis™ Optical EMS application and Informix database and reboot the system.

Important! Before rebooting the Navis™ Optical EMS application using the Shutdown command as described below, the system console ***must*** be powered on.

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

1 Log in as `root` to the Navis™ Optical EMS host computer.

Result:

A # prompt is displayed.

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

(r=reboot, y=yes, 0=now)

END OF STEPS

□

Reinstall the HP OpenView License

Purpose

Use this procedure to reinstall the HP OpenView License.

Before you begin

Before you begin this task, you must complete the procedure ***Installing HP OpenView*** which is described in the *Navis™ Optical EMS Installation Guide.*

While doing this procedure, you will have to run scripts and access files. If the appropriate directories do not exist, you will have to create them.

After completing this procedure, follow the procedure ***Installing the HP OpenView License*** which is described in the *Navis™ Optical EMS Installation Guide* to install the HP OpenView permanent License.

Task

Complete the following steps to reinstall the HP OpenView License.

1 Log in as ***ems***.

2 Bring down the Navis™ Optical EMS application using the following command:

```
dn –x
```

3 Enter the following command:

```
cd /opt/OV/osiam/osiam26F
```

4 Enter the following command to stop any OpenView processes:

```
./stopATOSHPOV
```

5 Enter the following command:

```
su – (root)
```

6 Enter the following command:

```
ps –eaf | grep –i ov | grep –v grep
```

Result:

The resulting output of this command should not return an active process.

7 Enter the following command:

```
ps –eaf | grep ftr | grep –v grep
```

Result:

The resulting output of this command should not return an active process.

If the output of this command returns a process(es), then execute the following command for each process:

```
kill –9 <PID from pf>
```

8 Enter the following command:

```
cd /var/opt/ifor
```

9 Enter the following command to rename the nodelock file:

```
mv nodelock onodelock
```

10 Enter the following command to rename the .instant file:

```
mv .instant o.instant
```

11 Enter the following command to remove the OpenView License:

```
swremove OVLicenseSvrHP10
```

12 Enter the following command to remove the OpenView DM5.03 PF3000 Migration:

```
swremove PHSS_16027
```

13 Enter the following command to remove the OpenView DM5.03 PMD select fail fix:

```
swremove PHSS_21580
```

14 Enter the following commands to remove the DM TMN Agent Platform:

```
swremove DMEngHPux10x
```

15 Enter the following command:

```
mv /etc/snc.rc /etc/osnc.rc
```

16 Enter the following command to mount the CD to the CDROM drive:

```
mount /dev/cdrom /cdrom
```

17 Enter the following command:

```
cd /cdrom
```

18 Enter the following command:

```
export TERM=vt100
```

19 Enter the following command:

```
./install.ots
```

20 After the system has rebooted, log in as `root`.

21 Enter the following command:

```
mv /etc/osnc.rc /etc/snc.rc
```

22 Enter the following command:

```
mount /dev/cdrom /cdrom
```

23 Enter the following command:

```
cd /cdrom
```

24 Enter the following command:

```
./install
```

25 Enter the following command:

```
/tmp/installPF3000
```

26 Follow the procedure ***Installing the HPOpenView License*** in the ***Navis™ Optical EMSInstallation Guide*** to install the HP OpenView permanent License.

27 Run the `installEms` script and choose option 5, Configure EMS, using the profile saved from the last session.

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 EMSdatabase 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

Back Up the Navis™ Optical EMS Database

Purpose

Maintaining tape backups of the database is critical to the overall reliability of Navis™ Optical EMS. 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 items as you prepare for database backups:

- You must be able to physically access the Navis™ Optical EMS host computer to insert and remove backup tapes.
- The database should be backed up at least once a week (more frequently when disk activity is high).
- In addition to the above recommendations, a backup should be verified and saved permanently off-site every six months. This is an additional safeguard against problems resulting from a faulty tape and/or tape drive.
- A Navis™ Optical EMS database backup requires one or more tapes depending upon the size of the database.
- Be sure to label backup tapes with the date and contents of the tape as instructed by the Informix backup and restore processes.
- Restoring the Navis™ Optical EMS database requires that you bring the Navis™ Optical EMS system down and take the Informix database program off-line.

Task

Perform the following steps to back up the Navis™ Optical EMS application.

1 Insert a tape into the tape drive of the Navis™ Optical EMS host computer.

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

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

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

Important! An archive 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 archive 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 Database

Task **Important!** The Navis™ Optical EMS application ***must*** be down to execute the restore procedure, and you ***must*** have the same database configuration.

The following procedure is used for restoring the Navis™ Optical EMS database.

1. Log into the Navis™ Optical EMS host as ***ems***.

2. Bring the Navis™ Optical EMS application down by typing `dn –x` and pressing the Return/Enter key at the system prompt.

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

4. Make sure 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 Return/Enter key to bring the Informix server offline.

6. To start the restore process, type `ontape -r` at the system prompt and press the Return/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 Return/Enter key to put Informix in online mode

8 To confirm Informix is in online status, type `onstat -` and press the Return/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 back to ***ems*** by typing `exit` and pressing the Return/Enter key.

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

END OF STEPS

□

Back Up Navis™ Optical EMS Application and DSA Data

Purpose Use this procedure to back up key Navis™ Optical EMS application data and database data, including NE directory information maintained by the Directory Services Agent (DSA). You have the option of backing up one database or set of application data at a time. You can back up the data to a single tape or multiple tapes.

Task Complete the following steps to do a backup of the desired application data or database data.

1 Insert a tape into the tape drive of the Navis™ Optical EMShost computer.

2 Log into the Navis™ Optical EMS host using the `ems` login.

3 At the UNIX prompt, enter the command`ems_backup`

The syntax of the command is:

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

where:

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

- `EMS` - Informix database
- `CF` - Configuration data
- `PM` - Performance Monitoring data
- `NQ` - Northbound CMISE data
- `NCI` - CORBA interface data

`-one` - back up all data onto one tape. Default is multiple tapes. If the `-one` option is used, you would insert one blank tape in the tape drive and execute the command ems_backup -one

`-app` - back up only application data and DSA data

Important! If no options are 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 overwriting of data.

Result:

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

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

END OF STEPS

□

Restore Navis™ Optical EMS Application and DSA Data

Purpose Use this procedure to restore key Navis™ Optical EMS application data and database data, including NE directory information maintained by the Directory Services Agent (DSA). You have the option of restoring one database or set of application data at a time. You can restore the data from a single tape or multiple tapes.

Task Complete the following steps to restore the desired application data or database data.

1 Log into the Navis™ Optical EMS host using the `ems` login.

2 At the UNIX prompt, enter the command `ems_recover`

The syntax of the command is:

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

where:

`-d` - restore one database from tape:

- `EMS` - Informix database
- `CF` - Configuration data
- `PM` - Performance Monitoring data
- `NQ` - Northbound CMISE data
- `NCI` - CORBA interface data

`-app` - restore only application data and DSA data from tape

END OF STEPS

□

Export the Navis™ Optical EMS Database to a Directory

Purpose A copy of the database can also be exported to an ASCII text format. This would allow you to transfer the database to another Informix environment that is configured differently.

Task **Important!** The Navis™ Optical EMS application ***must*** be shut down before doing a database export. Back up the /ems/dsa directory to ensure system consistency after a restart.

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

1 Log in as `ems`.

2 Bring the Navis™ Optical EMS application down.

3 At the UNIX prompt, use the following commands to back up the Navis™ Optical EMS 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 command with different n if n>1)

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

`dbexport $NQ_DBNAME -c -ss -o <directory>` (only for northbound CMISE)

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

4 After each DB export command, the message “dbexport complete” indicates the procedure has been successfully completed.

END OF STEPS

□

Export the Navis™ Optical EMS Database to Tape

Procedure The following procedure is used to perform a database export to tape.

1 Log in as `ems`.

2 Bring the Navis™ Optical EMS application down.

Important! Put in a new tape before executing each of the following commands. Each command may require more than one tape. Swap a tape by following the instruction from the prompt.

3 At the UNIX prompt, use the following commands to back up the Navis™ Optical EMS database to tape.

```
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 command with different n if n>1.

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

`dbexport $NQ_DBNAME -c -ss -t /dev/rmt/0m -b 512 -s 2000000` (only for northbound CMISE)

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

4 After each DB export command, the message “dbexport complete” indicates the procedure has been successfully completed.

END OF STEPS

□

Import the Navis™ Optical EMS Database from a Directory

Purpose A copy of the database can also be "imported" from a database exported by `dbexport` (described previously).

Important! 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 The following procedure is used to perform a database import 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 command with different n if n>1.

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

If `get_dbmodel` returns SUPREME or SUPREME-N:

`dbimport $NQ_DBNAME -d nq1_dbs -c -i <directory>` (only for northbound CMISE)

Otherwise:

`dbimport $NQ_DBNAME -d fm2_dbs -c -i <directory><Enter>` (only for northbound CMISE)

If `get_dbmodel` returns SUPREME or SUPREME-N:

`dbimport $NCI_DBNAME -d nq1_dbs -c -i <directory><Enter>` (only for CORBA interface)

Otherwise:

`dbimport $NCI_DBNAME -d fm2_dbs -c -i <directory><Enter>` (only for CORBA interface)

Result:

After each DB import 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 command with different n if n>1).

`db_logging -U $PM_DBNAME`

`db_logging -U $NQ_DBNAME`

`db_logging -U $NCI_DBNAME`

END OF STEPS

□

Import the Navis™ Optical EMS Database from Tape

Task The following procedure is used to perform a database import from tape.

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 -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 command with different n if n>1.

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

If get_dbmodel returns SUPREME or SUPREME-N:

`dbimport $NQ_DBNAME -d nq1_dbs -c -t /dev/rmt/0m -b 512 -s 2000000` (only for northbound CMISE)

Otherwise:

`dbimport $NQ_DBNAME -d fm2_dbs -c -t /dev/rmt/0m -b 512 -s 2000000` (only for northbound CMISE)

If `get_dbmodel` returns SUPREME or SUPREME-N:

`dbimport $NCI_DBNAME -d nq1_dbs -c -t /dev/rmt/0m -b 512 -s 2000000` (only for CORBA interface)

Otherwise:

`dbimport $NCI_DBNAME -d fm2_dbs -c -t /dev/rmt/0m -b 512 -s 2000000` (only for CORBA interface)

Result:

After each DB import 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 command with different n if n>1).

`db_logging -U $PM_DBNAME`

`db_logging -U $NQ_DBNAME`

`db_logging -U $NCI_DBNAME`

END OF STEPS

□

5 Management Communication of Navis™ Optical EMS

Overview

Purpose

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

Contents

Configure OSI in the Navis™ Optical EMS Host

Purpose 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.

Task The following procedure is used for configuring OSI in the Navis™ Optical EMS host. The LAN card should be configured before running install.

1 Bring down the Navis™ Optical EMS application by typing `dn`.

2 su to root.

3 Get the number or MAC address of the LAN card by using lanscan. (This is also done automatically).

4 Run installEms.

5 Select option #4) Configure EMS - making the provisioned parameters effective.

Result:

You will be prompted to select the OSI configuration options.

Notes:

1. You will need a separate LAN card for the OSI LAN. There needs to be one LAN card for the Navis™ Optical EMSlocal LAN and another card for the OSI to Network Element communications.
2. It is also recommended that each LAN card is connected to a different hub, as the hubs can sometimes cause communication problems.

3. For LAN redundancy you will need 2 LAN cards for OSI. You should also put a separate hub for each LAN card for extra redundancy. (Remember you cannot use the workstation LAN card for redundancy. You will need to purchase another LAN card for OSI support.)
4. LAN Cards 0 and 1 are part of the HP machine. They can be found on the back of the host. The HP host counts LAN cards from top left to bottom right.
5. When using external LAN cards you must power down the machine and move the LAN card jumpers from INT to EXT. The front two jumpers should be on.
6. Both LAN cards should be on a different SUBNET.
   These are the IP LAN card and the Southbound LAN card.

END OF STEPS

Configure OSI and TCP/IP on Separate LAN Cards

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

As an example, suppose that we have 3 cards as seen below. We will use lan0 for OSI, lan1 for OSI over TCP/IP, and lan2 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 s nap2 3 ETHER Yes 119
```

Task The following procedure is used for configuring OSI and TCP over OSI communications on different network interfaces. The LAN cards should be configured before running install.

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 - making the provisioned parameters effective.

4 The following screen output is displayed.. User input to the screen prompts is shown in bold.

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 Attatchment 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

Set Up WaveStar® NCC

Purpose

Navis™ Optical EMS supports OSI connections with NEs over a TCP/IP backbone network. In OSI over TCP/IP communications, a WaveStar® NCC or WaveStar™ OLS 1.6T is required to perform OSI protocol conversion, as a transport bridge, for messages/responses handled to/from the EMS and NEs.

A WaveStar® NCC can be provisioned to serve two main functions:

- Directory Services Agent (DSA) for SONET Directory Services (SDS)
- Transport bridge for TCP/IP to OSI protocol conversion for OSI-connected WaveStar® BWM NEs communicating with Navis™ Optical EMS over a TCP/IP backbone network
  The Navis™ Optical EMS currently supports Release 1.0 through Release 3.2 of the WaveStar® NCC. Future releases of the WaveStar® NCC may not be supported by the Navis™ Optical EMSand the WaveStar® NCC product will be eventually phased out. The Directory Services Agent (DSA) functionality provided by the WaveStar® NCC will be assumed by the Navis™ Optical EMS. The TCP/IP Gateway NE (GNE) functionality currently provided by the WaveStar® NCC will be assumed by a WaveStar® BWM, a WaveStar® TDM 2.5G, or aWaveStar® TDM 10G, respectively, for these NE types to communicate with the Navis™ Optical EMS host.

If using a router instead of a Network Element, the router must be set up as follows:

- IS-IS Routing Protocol 10589
- TARP - TID Access Resolution Protocol (Bellcore standard GR-253 formerly TR-252)
- IEEE 802.3 Compliant
- OSI 7 layer stack

Task

The following commands can be issued at the WaveStar® NCC CIT in TL1 mode.

1 ## Set Upper Layer Stack - Layer 3 Parameters

```
ENT-ULSDCC-L3:NGN-NCC::189:::131v2is=enable;
ENT-ULSDCC-L3:NGN-NCC::192:::L3AREA=0030;
```

2 ## Set Upper Layer Stack Information - Layer 4

```
ENT-ULSDCC-L4:NGN-NCC::194:::141ftm=10
ENT-ULSDCC-L4:NGN-NCC::195:::141ftm=5;
ENT-ULSDCC-L4:NGN-NCC::196:::14etof=enable;
ENT-ULSDCC-L4:NGN-NCC::197:::14etpf=enable;
ENT-ULSDCC-L4:NGN-NCC::198:::14etrf=enable;
```

3 ## Retrieve Upper Layer Stack Information

```
RTRV-ULS:NGN-NCC::186 ;
```

4 ##Retrieve Upper Layer Stack Information - Layer 3

```
RTRV-ULSDCC-L4:NGN-NCC::193;
```

5 ## Retrieve Upper Layer Stack Information - Layer 4

```
RTRV-ULSDCC-L4:NGN-NCC::197;
```

6 ## Retrieve NE Level Parameters

```
RTRV-NE:NGN-NCC::210;
```

END OF STEPS

□

Configure WaveStar™ OLS 1.6T Transport Bridge

Task From the network element side the following commands are necessary to provision the WaveStar™ OLS 1.6T to be both a Transport Bridge and a Registration Manager.

1 Enter System command gives an IP address to the NE's OS port. Do this if the NE is going to be a transport bridge.

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

Example:

The following is an example. It is on separate lines only to make it easier to read:

ENT-SYS:WSOLS400G-----12345678-::XXX:::
IP_ADDRESS=123.456.789.012,
DFLTRTR_IPADDRESS=123.456.789.012, LOCAL_SUBNET-MASK=255.255.255.0;

1. The IP address is the IP address given to the Network Element by the network administrator.
2. The dfltrtr ip address is the IP address of the default gateway.
3. The NE will reset if the subnet mask is entered.

2 Enter the Registration Manager (RM). One one RM is needed per OSI area.

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

Example:

The following is an example. It is on separate lines only to make it easier to read:

ENT-RMA:WSOLS400G-----12345678-:SYSTEM:XXX1:::
RM_ACTIVE=ENABLE,DSA_PSEL=0123,
DSA_SSEL=012345, DSA_TSEL=012345,
PRI_DSA_NSAP=1339840F800000000000000000xxxxxxxxxxxx,

PREFIX_COUNTRY=US,PREFIX_ORG=LUCENT,
PREFIX_SUBORG1=EMS1;

1. The primary DSA NSAP is the NSAP of the Navis™ Optical EMS southbound LAN card prefixed with a 13 for a total of 40 characters. Use this parameter only if not using a transport bridge. This parameter is only used for pure OSI communications.
2. The PSEL, SSEL, and TSEL (presentation, session and transport layers) are the recommended values.

3 Enter Transport Bridge.

ENT-TSB:TID:SYSTEM:CTAG:::[spec_block]; This needs to be entered in addition to the ent-sys command.

ENT-TSB:WSOLS400G-----12345678-:SYSTEM:XXX:::
PRI_TSB_NSAP=1339840f800000000000000000000xxxxxxxxxxxx,
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 the NEs in the network should now register themselves with the Navis™ Optical EMS.

END OF STEPS

□

Configure CMISE Over Transport Bridge when Routers are Involved (WaveStar™ OLS 1.6T)

Task Complete the following steps to configure CMISE over a transport bridge.

1 Login as

```
root .
```

2 Create an alternate address as */etc/opt/OV/share/conf/ft_local_p_addr* by doing the following:

```
cd /etc/opt/OV/share/conf
```

3 Use text editor to edit *ft_local_p_addr*

```
vi ft_local_p_addr
```

4 Find the line with HOST IP address by the following:

- identify the line ending in ":1006". An example line is as below: OVDM,ses0,tp0,0x5400728722031720100101000102400001:1006
- the 12 characters preceeding "0102400001" are the HOST IP address; so the HOST IP address from the example line is 172.10.10.100.

5 Replace the original host IP address with the router translated IP address and make sure the IP address is 12 characters long and using leading zeroes where necessary.

Important! The format of the file is really sensitive, so please take extra caution when you do any modification.

6 Save the file.

7 Login as `ems` and bring the Navis™ Optical EMSdown then up or restart all Q3 managers (i.e. SB_Q3_400g01, SB_Q3_400g02, etc) to take effect.

8 Do the following verification after system is restarted:

- login as `ems`
- type in `sb400goam`
- under ----> prompt, type in “address <TID>”; any valid <TID> can be used
- the IP address displayed under TCPIP of File Transfer should be the same address as entered in the *ft_local_p_addr*
- type in `quit` to exit sb400goam
- done

END OF STEPS

□

Set Up X.25 Global Link Settings

Purpose The global link settings are, normally, Line Speed, Synchronous Timing Source, and Virtual Channel characteristics. These are Level 2 specifications that are used to gain the “synchronization” needed before data can be sent.

Task Complete the following steps to set up X.25 global link settings.

1 Log in as `root`.

2 Get the physical address of the Mux interface cards by typing the following command:

```
ioscan -f | grep acc
```

3 The global links file (sometimes called the “answer file”) must be set up. It can be found in the following directory. (HP-UX Rel 11.0)

```
cd /opt/acc/cfg/
```

4 Next you will vi the x25_config.answ file and define the physical address of the Mux card (see above for the correct address). Below is a small part of the x25_config.answ file.

Interface-Definition

* mx# bus#:slot#

Mux 0 10:4:4 /opt/acc/mux/abs/x25.zabs

Mux 1 10:4:12 /opt/acc/mux/abs/x25.zabs

5 Now it is time to configure the timing source and the line speed. Ports 0 through 7 have been set for external timing and a line speed of 57600 (56k) using a V35 mux interface panel. If using the RS232 Mux interface panel, the line speed must be configured as 9600, as the RS232 port cannot support 57600 and the mux interface panel listing shown as RS232. Below is a small part of the x25_config.answ file.

Port-Definition

Port 00:00 RS232 57600 Ext SDLC x1 NRZ

Port 00:01 RS232 57600 Ext SDLC x1 NRZ

Port 00:02 RS232 57600 Ext SDLC x1 NRZ

Port 00:03 RS232 57600 Ext SDLC x1 NRZ

Port 00:04 RS232 57600 Ext SDLC x1 NRZ

Port 00:05 RS232 57600 Ext SDLC x1 NRZ

Port 00:06 RS232 57600 Ext SDLC x1 NRZ

Port 00:07 RS232 57600 Ext SDLC x1 NRZ

6 The first line in each port's Terminal Definition defines the specific X.25 driver to use and its Logical Presence Type (DTE or DCE). For the Navis™ Optical EMS, always use the X.25.LAPB driver.

* device file: zx25m0p0 mux: 0 port: 0

* mknod zx25m0p0 c 125 0x0300 2>/dev/null

Term 0001 0:0 X25.LAPB 0000h 4BEAh 10 0 0 0 0 "L2 DCE"

no_autostart

7 The remaining lines in each ports Terminal Definition specifies the Virtual Channels on this link. The two (2) types of Virtual Channels used are ***x25.pvc*** and ***x25.svc.io***

8 Configure SVC communications. The following is an example:

Term 020 0:0 x25.svc.io 0000h 0200h 99 0 0 0 0 "L3 svc"

Term 021 0:0 x25.svc.io 0000h 0200h 99 0 0 0 0 "L3 svc"

.

.

.

9 Configure PVC communications. The following is an example:

Term 100 0:0 x25.pvc 0000h 0200h 99 0 0 0 0 "L3 pvc"

Term 101 0:0 x25.pvc 0000h 0200h 99 0 0 0 0 "L3 pvc"

.

.

.

END OF STEPS

Set Up X.25 Specific Link Settings

Purpose The ***etc/x25/x25_config.XX*** file defines the Level 3 characteristics of a specific X.25 port on the Navis™ Optical EMScomputer. There must be one of these files for each port you wish to use. These files are often referred to as the X.25 “config” files.

Procedure Complete the following steps to set up specific link settings.

1 The *etc/x25/x25_config.XX* file must be manipulated by hand using a text editor such as “vi”.

Example:

A sample file (with inserted comments) looks like:

#

X.25 Initialization File Created: Fri June 16, 1995#

#

Navis™ Optical EMS- AI LINK DEFINITION for Mux 0, Port 4#

#

Global Parameters

#

File: x25_config.04

Directory: /etc/x25

END OF STEPS

□

Set Up X.25 for LCT NE

Task To configure an SVC channel for use with the Navis™ Optical EMS, perform the following.

1. Log into the LCT using the CIT and Centerlink software.
2. From the menu select: **Security⇒Enter ⇒Channel Identifier⇒security**
3. From the menu, select the appropriate OS Type: MT, MA, CMDR, OTHR, RST, NONE (if using one SVC, you must select OTHR).
4. Enter svc calling address (CALLADDR).

END OF STEPS

Task To configure a PVC channel for use with the Navis™ Optical EMS, perform the following.

1. Log into the FT-2000 LCT using the CIT and Centerlink software.
2. From the menu select: **Security⇒Enter ⇒Channel Identifier⇒security**
3. Select **pvc**.
4. From the menu, select the appropriate OS Type: MT, MA, CMDR, OTHR, RST, NONE (if using one PVC, you must select OTHR).
5. Enter svc calling address (CALLADDR).

END OF STEPS

Table 5-1 Table of Channel Types

OS Type	Function
MT	maintenance all autonomous message but REPT DBCHG
MA	memory-admin all REPT DBCHG messages
CMDR	cmt-response no autonomous messages
OTHR	all autonomous messages
RST	all autonomous messages but REPT EVT
NONE	Nothing

Set Up OSI for WaveStar® BWM NE

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

The WaveStar® BWM NE uses the J175 or J177 DB9 connector for OSI communications. This 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 for a WaveStar® BWM NE.

1 To retrieve the current configuration:

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

2 To enter or change the configuraton:

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 for WaveStar® BWM NE

Purpose Use this procedure to configure a WaveStar® BWM NE for TCP/IP communications using the WaveStar® CIT.

The WaveStar® BWM NE uses the J175 or J177 DB9 connector for OSI communications. This 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 configure a WaveStar® BWM NE for TCP/IP communications.

1 Log into the NE using the WaveStar® CIT.

2 Enter the IP address in the WaveStar® BWM NE 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=TL1MEMORYADMI
```

For the `ACID`, the choices are:

- TL1MAINTENANCE
- TL1MEMORYADMINISTRATION
- TL1TEST

- TL1OTHERQ
- TL1PEERCOMM

END OF STEPS

Set Up OSI for WaveStar™ OLS 1.6T NE

Purpose The 400G uses the J32OS DB9 connector located in the system bay interconnect panel.

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

1 To retrieve the current OSI configuration:

```
RTRV-OSI:TID::ctag;
```

Example:

The following is an example of `retrieve` command.

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

IP 789012

<

OLS-400G 93-10-26 16:42:11

M 789012 COMPLD

"localaddress=39000080,isislvl=Level-2,drp=64"
```

2 To enter or change the OSI configuraton:

```
ENT-OSI:TID::CTAG:{GEN_BLOCK}{:{:{SPEC_BLOCK}}};
```

Example:

The following is an example of `enter` command.

```
ent-osi:tid::ctag:::localaddress=1339840f800000000000dddd99

IP 123456

<

400G 93-10-26 16:42:11

M 123456 COMPLD
```

END OF STEPS

□

Set Up LambdaRouter *LambdaRouter*™AOS

Procedure Complete the following steps to obtain and assign an IP address for a *LambdaRouter*AOS and to database this network element type in Navis™ Optical EMS.

1 Log into the *LambdaRouter*AOS CIT using the CIT default login and password:

CIT default login - LUC01

Default password - OXC+1

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 *LambdaRouter*AOS's IP address.

Result:

A separate window is displayed for selection of the system controller (DCC-1–1)

5 Select the system controller.

Result:

A separate window is displayed for inputting the IP address.

6 Input the IP address.

7 Click the OK button.

8 Log into Navis™ Optical EMS.

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 1-20 alphanumeric characters. Hyphens, slashes ("/"), and periods are allowed. This field is required.

15 Enter the NE's Alias. An alias can be 1-40 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's 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 no selection is 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 host via a GNE	the GNE radio button. Go to Step 19.
The NE is communicating directly with the Navis™ Optical EMS host 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 host 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, a *LambdaRouter*AOS allows you to enter a second IP address.

If two IP addresses are entered, Navis™ Optical EMS uses the first IP address to make a connection with the NE. If the first IP address fails for some reason, Navis™ Optical EMS 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 1-10 characters.

28 Enter the primary NE password for the NE login. An NE password must be 6-10 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 1-10 characters.

31 Enter the backup password for the NE. An NE password must be 6-10 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 Metropolis™ EON

Purpose Use this procedure to enable the LAN connection for a Metropolis™ EON using the network element's CIT.

Before you begin Before you begin this task, make sure that the Metropolis™ EON network element is connected to the J13 port on the front of the system.

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

1 Log into the network element's CIT using the CIT default login and password:

CIT default login - LT01

Default password - FT-2000

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 see if the LAN connection is enabled. If not, enable it.

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

5 Issue the following TL1 command to check OSI communications:

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

Result:

Output from the TL1 command issued should be similar to the following (sample is for a Metropolis™ EON NE):

`Local= 39840f800000000000000000000`***Note: Org, Routing Domain, Area Addresses***

`open_sid= 08006a0643db` ***Note: MAC address of the OLS 40G/80G***

`prov_sid= 000000000000` ***Note: Should always be zeros***

`lanisislvl= Follow-Node` ***Note: Should always be follow-node***

`nodeisislvl= 2` ***Note: this line should be set to Level 1 or 2***

`transfermode= uits` ***Note: should always be uits***

END OF STEPS

Set Up Metropolis™ DMX (TCP/IP Communications)

Purpose Use this procedure to enable the LAN connection for a Metropolis™ DMX NE using the network element's CIT.

Before you begin Before you begin this task, make sure that the Metropolis™ DMX network element is connected to the J16 port on the rear panel of the system using an RJ 45 connector.

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

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

CIT default login - LUC01

CIT default password - DMX2.510G

CIT backup login - LUC02

CIT backup password - DMX2.510G

2 Enter the following command:

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

3 To set up a Metropolis™ DMX for IP connectivity, enter the following commands:

```
ENT-IPMAP:DMXTID::CTAG:::TCPIPADDR=xxx.xxx.xxx.xxx,ACID=TL1OTHER
```

The above command specifies the IP address of the NE

```
ENT-IPMAP:DMXTID::CTAG:::TCPIPADDR=xxx.xxx.xxx.xxx,TCPIPHOST=EMS
```

The above command specifies the IP address of the Navis™ Optical EMS host

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

END OF STEPS

□

Set Up Metropolis™ DMX (X.25 Communications)

Purpose Use this procedure to set up X.25 communications for aMetropolis™ DMX NE using the network element's CIT.

Before you begin Before you begin this task, make sure that the Metropolis™ DMX network element is connected to the J10 port on the rear panel of the system using an RS232 connector.

Task Complete the following steps to set up X.25 communications for an Metropolis™ DMX NE using the CIT.

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

CIT default login - LUC01

CIT default password - DMX2.510G

CIT backup login - LUC02

CIT backup password - DMX2.510G

2 Enter the following command:

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

3 Enter the following command:

```
ENT-OSACMAP:DMXTID:X25:CTAG::SVC:ACID=TL1OTHER,SNPA=1234567890;
```

In the above command, SNPAis the SVC calling number. SVCis the switched virtual circuit. If you specify a permanent virtual circuit (PVC), eliminate the SNPA number.

END OF STEPS

□

Set Up Metropolis™ DMX (OSI Communications)

Purpose Use this procedure to set up OSI communications for aMetropolis™ DMX NE using the network element's CIT.

Before you begin Before you begin this task, make sure that the Metropolis™ DMX network element is connected to the J16 port on the rear panel of the system using an RJ-45 connector.

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

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

CIT default login - LUC01

CIT default password - DMX2.510G

CIT backup login - LUC02

CIT backup password - DMX2.510G

2 Enter the following command:

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

3 Enter the following commands:

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

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

In the above command, SPEC_BLOCK refers to the Spec Block identifier as follows:

L3ORG - 6 digit Org Number

L3RES - 4 digit reserved

L3RD - 4 digit Routing Domain

L3AREA - 4 digit Area

L3LV2IS - Level 2 Routing Enabled/Disabled

END OF STEPS

□

6 Trouble Clearing

Overview

Purpose

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

Contents

Check the Status of the Navis™ Optical EMSApplication

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

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 lists the demon name, process ID (pid), process name, run status (option), persistance, and number of respawns of each application process.

The Navis™ Optical EMS processes are as follows:

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

If the application is down, the following message is displayed:

```
CURRENT RUN LEVEL IS: Shutdown
```

3 There are three states for the application:

- Shutdown —The Navis™ Optical EMS application is not up.
- Administrative —The Navis™ Optical EMSapplication is in transition (coming up or going down).
- Running —The Navis™ Optical EMSapplication is up.

The `Respawns` field should be 0 for every process. If any of these fields has a number larger than 0, then that process terminated and automatically restarted for some reason.

The `Pid` field should have a number greater than 0 for every process. If any of these fields has a 0, then that process terminated and is no longer running. The application must be restarted.

4 If you execute the `appstat` command, everything may look normal but the process may not be bound to Orbix. The `psit` command shows you if the appstat is true. At the UNIX prompt, enter the command `psit | more` to see if the process is running and bound to Orbix.

END OF STEPS

□

Check the Status of Stopped Process

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

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

1 Log in as `ems`.

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

Result:

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

END OF STEPS

□

Check the Communication Status of NEs

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

Task Complete the following steps to check the communication status of managed network elements

1 Log in as `ems`.

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

Result:

The system displays output that shows, for each NE:

- The communications port
- The NE's TID
- A communications active flag (Y = Yes)
- The communications type
- The communications channel ID
- The communications link status (Up or Down)
- The NE's login status (On or Off)

END OF STEPS

□

Activate a Network Element

Purpose Use this procedure to activate a network element

Related information To see the complete list of `cmtool` features that can be utilized, at the UNIX prompt, enter the command `cmtool -l`. The `cmtool` command can provide:

1. All GNE LinkStatus
2. One NE LinkStatus
3. One GNE LinkStatus
4. NE Activate/Deactivate
5. Resync config file
6. Switch primary/backup GNEs
7. Change 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

Task Complete the following steps to activate a network element.

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

Result:

The system displays output indicating that a new NE connection has been made and the IP address of the NE

END OF STEPS

Deactivate a Network Element

Purpose Use this procedure to deactivate a network element.

Task Complete the following steps to deactivate a network element.

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

Result:

The system displays output indicating that a deactivate process has been invoked and the IP address of the NE

END OF STEPS

□

Check Logged In Users

Purpose Use this procedure to show the present GUIs, the logged in users, and from which IP address they are logged in.

Task Complete the following steps to check the number of GUI clients currently running on the Navis™ Optical EMS host, the user login(s) for each GUI, and information about all queues.

1 At the UNIX prompt, enter the command

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

Result:

The system displays output indicating that a connection has been made to the GUI server and the GS prompt.

2 At the GS> prompt, enter `?`

Result:

The system displays the HELP menu for the `GUI_PROBE` command that shows the list of command option you can issue to obtain information

3

TO...	DO THIS...
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
Show information about all the queues	Enter `queues` at the GS> prompt
Exit the `GUI_PROBE` program	Enter `exit` 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 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. 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 steps to retrieve the Informix software release version.

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

Result:

The system displays messages indicating 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 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 show up, the system may be experiencing some congestion. 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 Informix database space usage.

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

Important! Verify that the free column for the dbspace partitions is not approaching 0. If it is, it indicates that the database is running out of free space. Use `add_dbs dbspacename` to add additional 10M to the dbspace specified. Verify again by `onstat -d`. The application does not have to be brought down to add dbspace.

Result:

The system displays output indicating the current Informix software release version, the dbspaces, and the chunk usage information.

END OF STEPS

□

Check Informix Error Codes

Purpose Use this procedure to display error codes and text for Informix errors.

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 display Informix error codes and 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

□

Check Level 2 Status of X.25 Network Connections

Purpose Use this procedure to display the status of each X.25 port on the Navis™ Optical EMS host.

Task Complete the following steps to display the status of each X.25 port on the Navis™ Optical EMS host.

1 At the UNIX prompt, enter the command `X25_check [Mux #]`

where *[Mux #]* is an optional parameter (0 to 3).

The default = 0 (MUX Card 0).

Important! The first four lines indicate the low-level X.25 processes are running; they should all have a status of UP. If any of the X.25 processes report a status of ***DOWN***, the X.25 connection needs to be restarted.

Result:

The system displays output indicating the status of each X.25 port.

The second section of the message, titled X.25 Port Status, displays the current Level 2 synchronization status for each link.

- Up— indicates the Navis™ Optical EMS host has synchronized with the PSN connected to this port.
- Down —indicates that Level 2 synchronization cannot be achieved on this port.

Check the following:

1. Is a Synchronous Modem Eliminator required?
2. Is the timing source set correctly in the X.25 answer file? For HP-UX Release 10.0, this file is found under */opt/acc/cfg/x25_config.answ*
3. Is the Data Rate set properly?
4. Have the Level 3 DTE/DCE network types been set properly in the X.25 *answer* file and specific X.25 *config* file?
5. Does the PSN support a V.35 interface?
6. Is the V.35 cable good?
7. Is the V.35 cable connected to the correct port?

END OF STEPS

Check Level 3 Status of X.25 Network Connections

Purpose Use this procedure to obtain various levels of detail about a specific X.25 port.

Task Complete the following steps to obtain various levels of detail about a specific X.25 port.

1 At the UNIX prompt, enter the command `x25stat -d [device_file] [options]`

where *[device_file]* is of the form */dev/zx25MMPP*

Important! Refer to Table 6-1, “Device Files for X.25 Ports.” (6-18) for a listing of device files for X.25 ports.

Result:

Result: The system displays lines of detail about the specified X.25 port.

Example:

dev/zx25m0p0

The last four characters indicate the MUX Card (MM) and Port Number (PP) to report on.

END OF STEPS

□

Check the Virtual Channel Status of an X.25 Port

Purpose Use this procedure to obtain the status of virtual channels on a specific X.25 port.

Task Complete the following steps to obtain the status of the virtual channels for a specific X.25 port.

1 At the UNIX prompt, enter the command `x25stat -d` *`device_file`*

where *`device_file`* is of the form */dev/zx25MMPP*, for example: */dev/zx25m0p0*

The last four characters indicate the MUX Card (***MM***) and Port number (***PP***) to report on.

In the example above, MUX Card 0, Port 0 (Connector J0) has been specified.

Refer to Table 6-1, “Device Files for X.25 Ports.” (6-18) immediately following this procedure for a listing of device files for X.25 ports.

Important! If the x25stat command is run on a port that is not connected to a PSN or is not configured properly, you will see the following message: x25stat WARNING: Level 2 is DOWN Check the following:

1. Were the right MUX and Port queried?
2. Does the PSN support a V.35 interface?
3. Is the V.35 cable connected to the right port on the PSN?
4. Is the V.35 cable connected to the right port on the Navis™ Optical EMS computer?

Result:

The system displays output that indicates, for each virtual channel of the specified X.25 port, the virtual channel type, the local address, its foreign address (if applicable), the virtual channel number, and whether it is currently connected.

All channels of VC type PVC appear whether they are in use or not. If the `Local Address` field has dashes, the PVC is defined but not actively in use. If the `Local Address` field has an X.121 Address displayed (this had been previously defined in the X.25

config file for this port), then the PVC has been restarted and communication ***may*** be established.

SVC channels that are currently in use appear after the last PVC channel. If no SVC channels are in use, then none are reported. However, they still are defined.

The above display shows that PVCs 3 and 8 have been reset and ***may*** be in use. SVC 20 is active and connected to X.121 address 9089492000.

END OF STEPS

The following table provides a listing of device files for all possible ports (if equipped)

Table 6-1 Device Files for X.25 Ports.

	MUX Card 0	MUX Card 1	MUX Card 2	MUX Card 3
Port 0:	/dev/zx25mop0	/dev/zx25m1p0	/dev/zx25m2p0	/dev/zx25m3p0
Port 1:	/dev/zx25m0p1	/dev/zx25m1p1	/dev/zx25m2p1	/dev/zx25m3p1
Port 2:	/dev/zx25m0p2	/dev/zx25m1p2	/dev/zx25m2p2	/dev/zx25m3p2
Port 3	/dev/zx25m0p3	/dev/zx25m1p3	/dev/zx25m2p3	/dev/zx25m3p3
Port 4:	/dev/zx25m0p4	/dev/zx25m1p4	/dev/zx25m2p4	/dev/zx25m3p4
Port 5:	/dev/zx25m0p5	/dev/zx25m1p5	/dev/zx25m2p5	/dev/zx25m3p5
Port 6:	/dev/zx25m0p6	/dev/zx25m1p6	/dev/zx25m2p6	/dev/zx25m3p6
Port 7:	/dev/zx25m0p7	/dev/zx25m1p7	/dev/zx25m2p7	/dev/zx25m3p7

Obtain X.25 Virtual Channel Non-Data Packet Statistics

Purpose Use this procedure to obtain virtual channel non-data packet statistics for a specific X.25 port.

Task Complete the following steps to obtain virtual channel non-data packet statistics for a specific X.25 port.

1 At the UNIX prompt, enter the command `x25stat -d` *`device_file -p`*

where *`device_file`* is of the form */dev/zx25MMPP*, for example: */dev/zx25m0p0*

The last four characters indicate the MUX Card (***MM***) and Port number (***PP***) to report on.

In the example above, MUX Card 0, Port 0 (Connector J0) has been specified.

Refer to Table 6-1, “Device Files for X.25 Ports.” (6-18) for a listing of device files for X.25 ports.

Important! VC 8, however, shows no current user. Even though the display in the previous section showed PVC 8 was connected, the fact is, the VC was successfully reset but no further data was exchanged on the channel.

Result:

Result: The system displays output that indicates, for each virtual channel of the specified X.25 port, the virtual channel state the current virtual channel user, the number of interrupt messages generated, and the number of resets.

All channels appear as in the previous section except that the VC type is not specified. The `VC User` is the protocol that is active on this virtual channel.

In the display above, VCs 3 and 20 have an active Level-3 (packet level) Programmatic Access user on them. This indicates that a machine is sending and receiving X.25 data over these channels. The next section will give you a clearer picture of this.

END OF STEPS

□

Obtain X.25 Virtual Channel Data Counters

Purpose Use this procedure to obtain the status of the virtual channel data counters on a specific X.25 port.

Task Complete the following steps to obtain the status of the virtual channel data counters on a specific X.25 port.

1 At the UNIX prompt, enter the command `x25stat -d device_file -t`

where `device_file` is of the form */dev/zx25MMPP*, for example: */dev/zx25m0p0*

The last four characters indicate the MUX Card (***MM***) and Port number (***PP***) to report on.

In the example above, MUX Card 0, Port 0 (Connector J0) has been specified.

Refer to Table 6-1, “Device Files for X.25 Ports.” (6-18) for a listing of device files for X.25 ports.

Important! VC 8, however, appears to be having a problem. Messages have been transmitted, but none received. The first display in the previous section showed VC 8 was connected. The next sections provide a more accurate picture. There is no current user because the VC is not transmitting ***and*** receiving data in both directions. Check the following:

- If the VC is a PVC:

1. Has the PVC been mapped correctly through the PSN?
2. Is the Navis™ Optical EMSusing the right PVC?

- If the VC is an SVC:

1. Is the Called X.121 Address correct?

- Other items to be checked (if attempting `pvctest` or `svctest`):

1. Is the TID of the NE correct?
2. Is the NE connected to the PSN?

Result:

The system displays output that indicates, for each virtual channel of the specified X.25 port, the virtual channel state, the

number of inbound messages, the number of outbound messages, the number of inbound data packets, the number of outbound data packets, and the number of inbound octets.

All channels appear as in the previous sections and the VC type is not specified.

In the sample output above, `Imsgs`, `Ipackets`, and `Ioctets` refer to messages ***received*** over the X.25.

`Omsgs`, `Opackets`, and `Ooctets` refer to messages ***transmitted*** over the X.25.

In the display above, VCs 3 and 20 appear to have traffic flowing in ***both*** directions. Typically, there are more messages received than transmitted. As the Navis™ Optical EMS system sends single commands to the NEs, the responses are sometimes long and received in several pieces (packets).

END OF STEPS

□

Reset an X.25 MUX Port

Purpose Use this procedure to reset a specific X.25 port without disrupting other data communications links.

Task Complete the following steps to reset a specific X.25 MUX port.

1 Log in as `root`, or `su` (super-user).

2 At the # prompt, enter the command `/usr/sbin/x25stop` *`device_file`*

where *`device_file`* is of the form: `/dev/zx25MMPP`, for example: `x25stop -d /dev/zx25m0p4`

This shuts down MUX Card 0, Port 4. You may specify any MUX/Port equipped in the computer.

There is no output to this command.

3 At the # prompt, enter the command: `/usr/sbin/x25init -c /etc/x25/x25_config.` *`MP`*

where *`MP`* is the MUX Card and Port Number, for example: `x25_config.04` identifies MUX Card 0, Port 4.

This re-initializes MUX Card 0, Port 4. You may specify any MUX/Port equipped in the computer.

Important! If there was a failure or inconsistency of some kind, you will receive an error message. Check the following:

- Refer to the HP-UX NACC X.25 section and verify that the relationships between the X.25 ***answer*** file and this X.25 ***config*** file are correct.
- It is possible that restarting a link may not work even though everything appears to be set up properly.
  In that case, it is best to restart the X.25 processes again. Refer to the procedure "Restart X.25 Processes" (6-23).

END OF STEPS

□

Restart X.25 Processes

Purpose Use this procedure to reset the X.25 communications server to clear potential communications problems. Restarting the X.25 communications server drops all connections to the Packet Switched Network (PSN) and re-restablishes the connections.

Task Complete the following steps to reset the X.25 communications server.

1 Log in as `root` or `su` to `root`.

2 At the # prompt, enter the command `/etc/x25/x25_config.rc`

Result:

The system displays messages indicating that the X.25 communications server processes are being brought down and then restarted. The X.25 server output is directed to the */usr/adm/x25server.log* file.

END OF STEPS

□

Deactivate/Reactivate System Links to Gateway Network Elements

Purpose Use this procedure to deactivate and then reactivate communications links with an X.25-connected Gateway Network Element (GNE). This procedure should be used if the various procedures for troubleshooting X.25 communication problems have failed to identify the source of the problem and recover communications. The problem may be a "hang" in the system X.25 drivers. This can occur if a PVC link to an NE is lost. This procedure can be used to remove the X.25 "hang".

Related tasks

- "Check Level 2 Status of X.25 Network Connections" (6-15)
- "Check the Virtual Channel Status of an X.25 Port" (6-17)
- "Obtain X.25 Virtual Channel Non-Data Packet Statistics" (6-19)
- "Obtain X.25 Virtual Channel Data Counters" (6-20)
- "Reset an X.25 MUX Port" (6-22)
- "Restart X.25 Processes" (6-23)

Task Complete the following steps to deactivate and then reactivate communications links with an X.25-connected GNE.

1 Log in as `ems`

2 To deactivate system links, enter the command `cmtool -n <TID> -o d`

Repeat this step for any GNEs that have a communications problem

3 To reactivate system links, enter the command `cmtool -n <TID> -o a`

Repeat this step for all GNEs ***except*** for the failed one.

END OF STEPS

□

Obtain Virtual Circuit Information for Gateway Network Elements

Purpose Use this procedure to obtain Packet-Switched Network (PSN) information about X.25-connected GNEs.

Task Complete the following steps to obtain PSN information about X.25-connected GNEs.

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

Result:

The system outputs a listing of GNEs (by TID), the VC types used by each GNE, and the type of PSN used by each GNE.

END OF STEPS

□

Test Permanent Virtual Circuit Connection to a Network Element

Purpose

Use this procedure to test communication via a specified permanent virtual circuit (PVC) to a network element.

Once an NE has been entered into the Navis™ Optical EMS database, the application will automatically try to gain communication to that element.

Before you begin

If you wish to run a `pvctest` to a network element which has already been databased, you must first deactivate the network element using the `cmtool` command.

Related task

Use the following procedure to deactivate a network element

- "Deactivate a Network Element" (6-8)

Task

Complete the following steps to test communication via a specified permanent virtual circuit (PVC) to a network element.

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

Result:

The system displays messages about the `pvctest` utility and a prompt for the NE's TID.

2 Enter the NE's TID.

Result:

The system prompts for the X.25 port.

3 Enter the X.25 port.

Result:

The system prompts for the PVC number.

4 Enter the X.25 PVC number.

Result:

The system prompts for a privileged login.

5 Enter a privileged login (for example, LUC01).

Result:

The system prompts for the privileged login password.

6 Enter the password for the privileged login.

Result:

The system displays a message and a prompt for the NE type (the prompt identifies each NE type by number; for example, NE Type 1 equals a DDM-2000).

7 Enter the appropriate number for the NE type.

Result:

The system displays a menu of choices.

8 Select Menu Option 1 (**ACT-USER**).

Important! If you do not receive a response from the NE, press **Control C** or the Esc key to break out of the program. Check the following:

- Is the NE powered up and operational?
- Is the NE connected to the X.25 network?
- Is the TID of the NE set properly?
- Are the channel maps in the local PSN (on the Navis™ Optical EMS side) set correctly?
- Are the channel maps in the remote PSN (on the NE side) set correctly?

Result:

The system displays output for the ACT-USER command. If the command is successful, the system displays messages confirming that you have successfully tested the PVC channel to the selected NE. Go to Step 9.

9 Select Menu Option 2 (CANC-USER).

Result:

The system displays output for the CANC-USER command. If the command is successful, the system displays a message indicating that the command issued is completed.

10 Select Menu Option 99 (Exit).

END OF STEPS

□

Test Switched Virtual Circuit Connection to a Network Element

Purpose Use this procedure to test communication via a specified switched virtual circuit (SVC) to a network element.

Task Complete the following steps to test communication via a specified switched virtual circuit (SVC) to a network element.

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

Result:

The system displays messages about the svctest utility and a prompt for the NE's TID.

2 Enter the NE's TID.

Result:

The system prompts for the X.25 port.

3 Enter the X.25 port.

Result:

The system prompts for the X.25 X.121 address for the NE.

4 Enter the X.25 X.121 address for the NE.

Important! Time-out and sub-address parameters should be added to the end of the Calling Address. These only work on the command line. The default value for time-out is 30 and for sub-address is 1. Even though the Navis™ Optical EMS will work with one VC, software management will not. It must have the second channel.

Result:

The system prompts for a privileged login.

5 Enter a privileged login (for example, `LUC01`).

Result:

The system prompts for the privileged login password.

6 Enter the password for the privileged login.

Important! On occasion, you may receive an error message indicating the SVC call was not successful, such as “connection refused.” This would imply that there is a problem in the PSN trying to route the call. Check the following:

- Do the PVC and SVC definitions on the PSN match the PVC and SVC definitions on the host?
- Is the SVC Address translation in the PSN mapped correctly?

Result:

If the login and SVC Call Request was processed successfully by the PSN, the system outputs a menu listing for NE types.

7 Select Menu Option 1 (ACT-USER).

Important! If you do not receive a response from the NE, press **Control C** or the Esc key to break out of the program. Check the following:

- Is the NE powered up and operational?
- Is the NE connected to the X.25 network?
- Is the TID of the NE set properly?
- Are the channel maps in the local PSN (on the Navis™ Optical EMS side) set correctly?
- Are the channel maps in the remote PSN (on the NE side) set correctly?

Result:

The system displays output for the ACT-USER command. If the command is successful, the system displays messages confirming that you have successfully tested the PVC channel to the selected NE. Go to Step 8.

8 Select Menu Option 2 (CANC-USER).

Result:

The system displays output for the CANC-USER command. If the command is successful, the system displays a message indicating that the command issued is completed.

9 Select Menu Option 99 (Exit).

END OF STEPS

□

Monitor OSI Stack on the Navis™ Optical EMS Host

Purpose Use this procedure to monitor the OSI stack on the Navis™ Optical EMS host. Once the `osiopu` process is running, you can send TARP requests to network elements.

Task Complete the following steps to monitor the OSI stack on the Navis™ Optical EMS host.

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

Result:

The system outputs messages indicating that the `osipu` process has started and returns with a UNIX prompt.

2

TO...	ENTER THE COMMAND...
Send a TARP request to a specific network element	`tarp getnsap C <TID>` **Important!** There is a complimentary command to the tarp getnsap C command. The command is: `tarp gettid H` (nsap of the network element you would like the TID for) If output from the completed TARP request obtained from isssuing the above command shows that the origin is from TDC, you must flush the TDC cache.
Flush the TDC cache	`tarp tdc flush`

3

TO...	ENTER...
Exit the `osiopu` command session	`$exit`**Important!** You must exit the `osipu` session before bringing the Navis™ Optical EMS down and then up, or problems may occur.

END OF STEPS

□

Verify IP Addresses and Names

Purpose Use this procedure to verify network device IP addresses and names for Navis™ Optical EMShosts and workstations.

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.

Task Complete the following steps 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. Each line 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.

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 Take note of 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 packets of data to remote workstations and get them back.

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 tht 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" (6-34). 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 into 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 tht 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" (6-34) procedure.

2

IF...	THEN...
Pinging the workstation still fails	Reboot the workstation and router.
Trouble still persists	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 telneting and logging into the Navis™ Optical EMS server, change directory to the Navis™ Optical EMS GUI software directory and entering 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 Navis™ Optical EMS 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*. The Navis™ Optical EMS classpath should be defined for each Navis™ Optical NMS CLASSPATH definition.

12 Check F-interface configuration file for correctness and enable debugging. The F-interface configuration file is:

/jui/jnm/itm/southbound/ems/emsFint/emsFint.cfg.

Check to see whether each release in the configuration file maps to the correct GUI software directory. Once editing is complete, try again to launch the Navis™ Optical NMS interface via the controllers map and the VCIT menu item.

If the cut-through still fails, you will need to examine the Navis™ Optical NMS debug log to determine the problem. The name of the debug log is displayed at Navis™ Optical NMS startup time and the file is always located in the /jui/logs directory. If you examine the log immediately after the cut-through failure, then the debug output should be near the end of the log. Check the following:

- determine whether the configuration file was found by the software.
- whether the correct GUI software was being launched for the specified Navis™ Optical EMS host.

The log file contents should indicate whether the proper instance of the Navis™ Optical EMS GUI software is being launched. 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

Recover from WaveStar™ OLS 1.6T In-Service Upgrade Failure

Purpose

Use this procedure to handle in-service upgrade failures on a WaveStar™ OLS 1.6T NE.

An in-service upgrade failure occurs when, in the last step in an in-service upgrade of the WaveStar™ OLS 1.6T NE from NE Release 5.0 to NE Release 6.0, the Activate NE Software process did not complete. The root cause of the failure is in the NE. Two failure scenarios are possible:

Two failure scenarios are possible:

- All of the provisioned data was preserved on the NE
- All of the provisioned data was lost on the NE

Related task

See " In Service Upgrade of WaveStar™ OLS 1.6TSoftware from Release 5.0 CMISE Mode to Release 6.0 TL1 Mode" in the *Navis™ Optical EMS Provisioning Guide.*.

Task

Complete the following steps to correct in-service upgrade failures for an OLS 400G NE.

1

IF...	THEN...
All of the provisioned data is preserved on the NE	Use the CIT to manually run the NE Release 6.0 software.
All of the provisioned data was lost on the NE	Manually re-install the NE Release 5.0 software via the flash card. Then, use the CIT to manually restart the NE to run Release 5.0 software.

2 Using the Navis™ Optical EMS GUI Map window main menu, delete the NE from the system using **Administration->Network->Network Element->Delete NE**

3

IF...	THEN...
All of the provisioned data is preserved on the NE	Using the Navis™ Optical EMSGUI main menu on the Map window, re-add the NE to the system using **Administration->Network->Network Element->Add NE**. When adding the NE, select the “TL1 only”Communication Type.
All of the provisioned data was lost on the NE	Using the Navis™ Optical EMSGUI main menu on the Map window, re-add the NE to the system using **Administration->Network->Network Element->Add NE**. When adding the NE, select the “CMISE only”Communication Type.

4

IF...	THEN...
All of the provisioned data is preserved on the NE	Skip this step. The recovery is completed.

IF...	THEN...
All of the provisioned data was lost on the NE	Insert the DDS tape that contains the backup configuration information into the DDS tape drive of the Navis™ Optical EMS host. At the Navis™ Optical EMS shell prompt, enter the following command: `cd /ems/obr_root/Data/W400G`. Then enter this command: `tar xv` Using the Navis™ Optical EMS GUI main menu on the Map window, choose **Software Management->Restore->Regular Restore** to restore the provisioned configuration back to the NE. Then repeat the the regular in-service upgrade procedure described in the task " In Service Upgrade of WaveStar™ OLS 1.6TSoftware from Release 5.0 CMISE Mode to Release 6.0 TL1 Mode" in the *Navis™ Optical EMS Provisioning Guide* starting from the Software Download step of that procedure.

END OF STEPS

□

7 Cluster Administration GUI Operations

Overview

Purpose

This chapter describes procedures related to the Navis™ Optical EMS cluster administration GUI. The cluster administration GUI is a separate GUI that is used to monitor geographically redundant Navis™ Optical EMS servers and to perform switchovers between Navis™ Optical EMS servers, as necessary.

Before you begin

Read Chapter 9, "Cluster Administration GUI for Geographically Redundant Navis™ Optical EMS Servers" to acquire a basic understanding of the Security Management features provided by Navis™ Optical EMS.

Contents

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 5.1).

IF...	ENTER...
It is a Windows-based system	`cd \emsR5.1`
It is a UNIX-based system	`cd <emsR5.1 home directory>`

3 Execute the cluster launch script, indicating the name of a single (any) Navis™ Optical EMS 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 will only be prompted for a login if you execute a menu item. By default, the system will display 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 (Cluster Administration GUI)

Purpose Use this procedure to configure the cluster administration GUI's email server.

Before you begin Before you begin this task, you must start up and log into the cluster administration GUI.

Be aware that 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" (7-3)

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:

Result: The mail server is defined for routing email.

END OF STEPS

□

Add a New Email User (Cluster Administration GUI)

Purpose Use this procedure to add a new user email account for the cluster administration GUI.

Before you begin Before you begin this task, you must start up and log into the cluster administration GUI.

Be aware that the list of email users is saved on the active host and then replicated to all standby hosts. Therefore, email user information, retrieved for the Manage Email Information window, is retrieved from any communicating Navis™ Optical EMS server. However, when saving new email information, new email user information will only be 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" (7-3)

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 Click the Add button on the Manage Email Information window.

Result:

The Email Account Information window is displayed.

4 Under **User Name**, enter the user name for the new email user. Any ***unique*** value may be entered for this field.

5 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.

6 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.

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

END OF STEPS

□

Modify User Email Information (Cluster Administration GUI)

Purpose

Use this procedure to modify user email account information for the cluster administration GUI.

Before you begin

Before you begin this task, you must start up and log into the cluster administration GUI.

Related tasks

- "Start the Cluster Administration GUI" (7-3)
- "Add a New Email User (Cluster Administration GUI)" (7-7)

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 not logged in, you will be prompted for your login password.

3 Double-click to select a user from the user list.

4 Click the Modify button.

Result:

The Email Account Information window is displayed.

5 Change the User Name, Email Address, and/or Pager Address fields, as required.

6 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 (Cluster Administration GUI)

Purpose

Use this procedure to delete a user's email information from the cluster administraton GUI.

Before you begin

Before you begin this task, you must start up and log into the cluster administration GUI.

Related tasks

- "Start the Cluster Administration GUI" (7-3)
- "Add a New Email User (Cluster Administration GUI)" (7-7)
- "Modify User Email Information (Cluster Administration GUI)" (7-9)

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 not logged in, you will be prompted for your login password.

3. Double-click to select a user from the user list.

4. Click the Delete button. A pop-up window is displayed, asking if you really want to delete the user's email information.

5. Choose Yes to delete the user's email information.

END OF STEPS

□

View User Email Information (Cluster Administration GUI)

Purpose Use this procedure to view a user's email information for the cluster administration GUI.

Before you begin Before you begin this task, you must start up and log into the cluster administration GUI.

Related tasks

- "Start the Cluster Administration GUI" (7-3)
- "Add a New Email User (Cluster Administration GUI)" (7-7)
- "Modify User Email Information (Cluster Administration GUI)" (7-9)
- "Delete User Email Information (Cluster Administration GUI)" (7-11)

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 not logged in, you will be prompted for your login password.

3. Double-click to select a user from the user list.

4. Click the View button.

   Result:

   The Email Account Information window is displayed, showing the selected user's email account information.

5 Click the Cancel button to close the Email Account Information window.

END OF STEPS

□

Test User Email Information (Cluster Administration GUI)

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. In this case, the cluster administration GUI contacts its desginated mail server and requests deliver of email to each user on the user email list.

Email is sent from the Navis™ Optical EMS server when the server software detects an abnormal condition in the cluster. 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

Before you begin this task, you must start up and log into the cluster administration GUI.

Related tasks

- "Start the Cluster Administration GUI" (7-3)
- "Add a New Email User (Cluster Administration GUI)" (7-7)
- "View User Email Information (Cluster Administration GUI)" (7-12)

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 not logged in, you will be prompted for your login password.

3 Double click to select a user from the user list.

4 Click the TEST button.

Result:

Result: The Email Test window is displayed, with the user's email information, with a sample email subject and text message that is editable.

5

TO...	DO THIS...
Send a test message from the client workstation (GUI)	Click the GUI radio button.**Important!** In order 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 Navis™ Optical EMS server	Click the Navis™ Optical EMS server radio button.

6 Click the SEND button to send the test email message.

Result:

If the test email message is transmitted successfully, the system displays a message indicating that the message was sent successfully.

END OF STEPS

□

Set Up Automatic Switchover (Cluster Administration GUI)

Purpose

Use this procedure to set up automatic switchover.

The cluster administration GUI can be configured to perform automatic switchover when a failure condition is detected by the GUI.

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 the 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.

Before you begin

Before you begin this task, you must start up and log into the cluster administration GUI as user `itm` with a valid password.

Be aware that it is recommended that only a single custer administration GUI be configured with automatic switchover enabled. However, if two GUIs are enabled for automatic switchover, the second switchover request to the standby Navis™ Optical EMS server would be denied, because a switchover operation would already be in progress.

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:

Result: The Edit Automatic Switchover window is displayed.

3 Choose to enable or disable automatic switchover.

TO...	DO THIS...
Enable automatic switchover	Choose **Enable** from the option menu. If automatic switchover is enabled, go to step 4 to define a failure elapsed time.
Disable automatic switchover	Choose **Disable** from the option menu. (The default is **Disable**).

4 Enter a failure elapsed time.

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.

5 After making your choices, click the OK button.

END OF STEPS

□

Perform Manual Switchover (Cluster Administration GUI)

Purpose Use this procedure to perform a manual switchover from one server to another in the event of a failure condition.

Before you begin Before you begin this task, you must 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" (7-3)

Task Complete the following steps to perform a manual switchover.

1

TO...	DO THIS...
Perform a manual switchover using the Navis™ Optical EMS 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.**Important!** If a switchover operation cannot be performed, an error message is displayed. **Result:** 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

8 Security Management Concepts

Overview

Purpose

This chapter provides general information about controlling access to Navis™ Optical EMS and its managed network elements.

Objectives

This chapter explains how to do the following:

- Change user and NE passwords
- Set up users and their level of access to NEs, functions, and commands in Navis™ Optical EMS

Contents

Password Administration

Overview

The Navis™ Optical EMS GUI provides functions for administering user passwords and NE passwords.

Changing an EMS user's password

The Change Password function is the only Administration function that is available to the EMS application user. An EMS 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 Navis™ Optical EMS, the system enforces that the default password must be changed to a new password, and displays the Change Password window for changing it.

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 at this point. If the expiration period is reached, and the user does not change the password before attempting to log into the system, system access is denied.

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

An EMS user login, however, can only be changed by the Navis™ Optical EMS administrator. See "Users" (8-4) for additional information about changing EMS user logins.

Global password administration

NEs have default login/passwords that are defined at the manufacturer prior to shipment. The NE login/password is required by the EMS user 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 a large number of NEs, this can be a very time-consuming process.

The Global Password Administration feature, which is available only for Lucent Technologies NEs, through the GUI, allows you to change

the primary and/or backup passwords for a number of NEs at the same time. This feature allows global password change for:

- Individual NEs (by TID)
- All NEs
- NEs by type
- Aggregate (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.

Related tasks

See the related tasks in Chapter 2, “Security Management”.

□

Network Security

Overview

The Navis™ Optical EMS system provides network security by allowing an administrator to define users and the extent of their access to NEs in the network and capability of performing certain functions and commands through the system.

Levels of access are defined by:

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

Users

A user is identified by a login and password and is provided access to the functions and features of the system as defined by the system administrator.

A user ID is defined for each user that accesses the system. The user ID (login) assigned to each user must be unique and contain 2-10 alphanumeric characters with no white spaces. When a user logs into Navis™ Optical EMS, 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 (as defined by the administrator), the user ID is automatically disabled and prohibited from logging into Navis™ Optical EMS. An “Invalid Login” message is displayed, an alarm is issued, and the user ID session is terminated.

The Navis™ Optical EMS system administrator can create, delete, and modify users (by user login) and their access permissions. Before any user can access the system, the user must be assigned a login and appropriate Target Group and Command Group access permissions.

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

When a user login is created by the administrator, it is initially set up with the following default values:

- User ID Login Type—GUI
- Password—no default password, must be entered by the administrator

- Command Group—Empty
- Target Group—Empty

Changing a user's 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 management

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

Through GUI functions, a Navis™ Optical EMS 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

The Navis™ Optical EMS generates a Minor alarm when any of the following 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

Any of the above conditions may indicate a possible threat or attempted breach of system security. A Minor alarm is generated against the application itself (TID=EMS) which can only be accessed by the EMS system administrator.

Related tasks

See the related tasks in Chapter 2, “Security Management”.

Command groups

A Command Group, also known as a user class, is a collection of EMS and NE commands that a specified user is allowed to enter through the system GUI. Each user is assigned to one and only one Command Group.

The system has a set of pre-defined Command Groups:

- Maintenance Command Group—This Command Group allows access to all Maintenance and Performance Management Category commands with Authorization Level 4 or less. (For an explanation of Authorization Levels, see the “NE logins” (8-7) section in this chapter.) This group of commands allows a user to view and modify all NE Maintenance information.
- Provisioning Command Group—This Command Group allows access to all Provisioning Category command with Authorization Level 4 or less. This group of commands allows a user to view and modify all NE provisioning information.
- Report-Only Command Group—This Command Group allows access to all categories of commands with Authorization Level 2 or less. (For an explanation of Authorization Levels, see the “NE logins” (8-7) section in this chapter.) This restricts a user to only being allowed to view NE information but not change it.
- General Command Group—This Command Group allows access to all categories of commands with Authorization Level 3 or less. This allows a user to view and modify most NE information.
- Privileged Command Group—This Command Group allows a user access to all categories of commands with Authorization Level 4 or less. (For an explanation of Authorization Levels, see the “NE logins” (8-7) section in this chapter.) This allows a user to view and modify almost all NE information, except for Administrator functions.
- All Command Group—This Command Group allows access to all commands, including Administrator functions supported by the NE. This is the super-user NE Command Group and is automatically assigned to the ***admin***logins; other user IDs may be assigned to this command group. It is usually reserved for the EMS administrator.
- Empty—This Command Group is set up with no commands.

The Navis™ Optical EMS system administrator can add, modify, or delete Command Groups. Additional Command Groups can be defined as needed by the administrator.

The system administrator can also copy the contents of an existing Command Group to a newly defined one.

Related tasks

See the related task in Chapter 2, "Security Management".

Target groups

A Target Group is a collection of NEs that a user can access. Together with Command Groups, Target Groups define user permissions and provide network security. Each user is assigned to one and only one Target Group.

The system has two pre-defined Target Groups:

- All Targets—provides access to all NEs in the network
- Empty—denies access to any NEs

The Navis™ Optical EMS administrator can add, modify, or delete Target Groups. Additional Target Groups can be defined as needed by the system administrator.

The system administrator can also copy the contents of an existing Target Group to a newly defined one.

Related tasks

See the related tasks in Chapter 2, "Security Management".

NE logins

Navis™ Optical EMS 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.

Navis™ Optical EMS allows you to define:

- NE logins
- Passwords for NE logins
- User Privilege Codes—a listing of exact permission levels to access functionality provided by the NE
- Temporary NE logins with an expiration date
- Copy of settings (User Privilege Codes) from another login (***Note: this does not include the ability to copy the login or password from another NE login***.)

- Password Aging/Expiration Time—the length of time (in days) that a password for an NE login can be used before it has to be changed to a new one
- User ID Status—Active or Suspended (some NE types)
- Inactivity Timeout—sets the timer for session inactivity before the system automatically times out
- Priority (some NE types)—sets the priority for logins

User privilege codes

When adding or modifying an NE login or copying another NE login's settings, a User Privilege Code is used to indicate the level of access to NE functions. A User Privilege Code is a combination of the Function Category and Authorization Level allowed.

The Functional Categories are as follows:

- ***Maintenance (M)*** - This Functional Category contains all of the Fault Management-related functions/features.
- ***Provision (P)*** - This Functional Category contains all of the Configuration Management-related functions/features.
- ***Performance Management (PM)*** - This Functional Category contains all of the Performance Management-related functions/features.
- ***Security (S)*** - This Functional Category contains all of the EMS Security and Administration-related functions/features.
- ***Test (T)*** - This Functional Category contains all of the Test Access-related features (applies to WaveStar BWM NEs only)

For Bandwidth Manager, 2.5G/10G, 10G/STM-64, and 10G (4–Fiber OC-192), the Functional Categories used are:

- ***Debug (D)***, ***Security (S)***, ***Maintenance (M)***, ***Provisioning (P)***, ***Performance Management (PM)***, and ***Test Access (T)***

For NCCs, the Functional Categories used are:

- ***Debug (D)***, ***Security (S)***, ***Maintenance (M)***, and***Provisioning (P)***

For LambdaRouter NEs, the Functional Categories used are:

- ***Security (S)***, ***Maintenance (M)***, ***Provisioning (P)***, and ***Test Access (T)***

For 40G/80G NEs, the Functional Categories used are:

- ***Security (S)***, ***Configuration (C)***, ***Fault (F)***, and ***Performance Management (PM)***

For DMX NEs, the following categories or privilege levels are used:

- ***Privileged*** - This Functional Category has user functions that are potentially service-affecting.
- ***General*** - This Functional Category has general Provisioning and Maintenance functions that are not service-affecting.
- ***Maintenance (M)*** - This Functional Category contains all of the Fault Management-related functions/features.
- ***Reports Only*** - This Functional Category only allows retrieve commands/functions.
- ***All*** - This Functional Category has Authorization Level 5 (the highest, equivalent to Super User) for all Maintenance, Provisioning, Performance Management, Security, and Test Access.

Each Functional Category has Authorization Levels consistent with NE privileges. The Authorization Levels are as follows:

- 1 - Empty (Lowest)
- 2 - Reports Only
- 3 - General
- 4 - Privileged
- 5 - Super User (Highest)

Important! The User Privilege Code on Super User NE logins cannot be modified.

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

Each NE must have at least one NE login with a Super User Authorization Level, to support any management task that may be required in the NE.

Example: user privilege code

The User Privilege Code “M3” indicates that a Navis™ Optical EMSuser login is authorized to execute all Maintenance Category functions with Authorization Level 3 or less. Therefore, the user

logging into an NE with this User Privilege Code is allowed to use the following EMS features:

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

Functions available by authorization level/functional category

The following table shows the functions/features that can be performed for each Authorization Level by Functional Category.

Table 8-1 Functions Available By Authorization Level/Functional Category

Auth. Level	Maintenance (M)	Provision (P)	Performance Management (PM)	Security (S)	TEST ACCESS (T)
1	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-EQPT, RTRV-EMS_ ALM-COM, RTRV-EMS_ ALM-STS12C,	RTRV-SNC_ ASSOC-OTPS		SAVE POSITIONS PREFERENCES, SAVE POSITIONS, SAVE PREFERENCES, RESTORE POSITIONS PREFERENCES, RESTORE POSITIONS, RESTORE PREFERENCES, COPY POSITIONS, COPY PREFERENCES, PRINT MAP, USER PREFERENCES, ALL ADMINIS-TRATION FUNCTIONS, ALL SECURITY, CHANGE PASSWORD, VIEW LOGS, VIEW ALL CMDRSP LOGS	

Table 8-1 Functions Available By Authorization Level/Functional Category (continued)

Auth. Level	Maintenance (M)	Provision (P)	Performance Management (PM)	Security (S)	TEST ACCESS (T)
1 (CONT'D)	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				

Table 8-1 Functions Available By Authorization Level/Functional Category (continued)

Auth. Level	Maintenance (M)	Provision (P)	Performance Management (PM)	Security (S)	TEST ACCESS (T)
2	VIEW ALARM MONITORING STATISTICS, ALL ALARM MONITORING STATISTICS, TL1 BROADCAST, TL1 MACRO BUILDER CUT-THROUGH	TL1 MACRO SCRIPTS, TL1 BROADCAST, TL1 MACRO BUILDER, CUT-THROUGH VIEW CROSS CONNECT, ALL CROSS CONNECTS, VIEW CROSS CONNECT EQUIPMENT, VIEW PATH, 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, ALL PM, VIEW PM DATA	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	LIST LOOPBACKS, LIST TEST ACCESS

Table 8-1 Functions Available By Authorization Level/Functional Category (continued)

Auth. Level	Maintenance (M)	Provision (P)	Performance Management (PM)	Security (S)	TEST ACCESS (T)
3	FILTER ALARMS RESYNCHRONIZE ALARMS, ALARM PROVISIONING ALW-SNC_ MSG-ALL, INH-SNC_ MSG-ALL	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		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	

Table 8-1 Functions Available By Authorization Level/Functional Category (continued)

Auth. Level	Maintenance (M)	Provision (P)	Performance Management (PM)	Security (S)	TEST ACCESS (T)
3 (CONT'D)		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,			

Table 8-1 Functions Available By Authorization Level/Functional Category (continued)

Auth. Level	Maintenance (M)	Provision (P)	Performance Management (PM)	Security (S)	TEST ACCESS (T)
3 (CON'TD)		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-STS3ENT-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			

Table 8-1 Functions Available By Authorization Level/Functional Category (continued)

Auth. Level	Maintenance (M)	Provision (P)	Performance Management (PM)	Security (S)	TEST ACCESS (T)
4	ALL ALARM MONITORING, ENABLE FULL ALARM MONITORING, ENABLE PARTIAL ALARM MONITORING, PROVISION PROTECTION SWITCH	ESTABLISH EQUIPMENT, REMOVE EQUIPMENT IP TUNNELING, DCC TERMINATIONS, DCC PROVISIONING	GLOBAL PM MGMT, NE PM MANAGEMENT	ADD AGGREGATE, ADD GNE ASSOCIATION, ADD NE, ADD SUBNET, ADD TRAIL, CHANGE AGGREGATE CONTENTS,	
4 (Cont'd)				DATE TIME MANAGEMENT, DELETE AGGREGATE, DELETE GNE ASSOCIATION, DELETE NE,	

Table 8-1 Functions Available By Authorization Level/Functional Category (continued)

Auth. Level	Maintenance (M)	Provision (P)	Performance Management (PM)	Security (S)	TEST ACCESS (T)
4 (Cont'd)				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,	

Table 8-1 Functions Available By Authorization Level/Functional Category (continued)

Auth. Level	Maintenance (M)	Provision (P)	Performance Management (PM)	Security (S)	TEST ACCESS (T)
4 (Cont'd)				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,	

Table 8-1 Functions Available By Authorization Level/Functional Category (continued)

Auth. Level	Maintenance (M)	Provision (P)	Performance Management (PM)	Security (S)	TEST ACCESS (T)
5				SCHEDULE SW COPY, SCHEDULE SW DOWNLOAD, RETRY INTERVALS, PROVISION DSA, DSA MANAGEMENTADD COMMAND GROUP, ADD TARGET GROUP,	
5 (Cont'd)				DELETE COMMAND GROUP, DELETE TARGET GROUP, MODIFY COMMAND GROUP, MODIFY TARGET GROUP, ADD USER,	

Table 8-1 Functions Available By Authorization Level/Functional Category (continued)

Auth. Level	Maintenance (M)	Provision (P)	Performance Management (PM)	Security (S)	TEST ACCESS (T)
5 (Cont'd)				MODIFY USER, DELETE USER, DISPLAY LOGGEDIN USERS, GLOBAL SECURITY PROVISIONING ADD NE USER, MODIFY NE USER, DELETE NE USER, RESET NE, PROCESSOR CONDITIONS	

TL1 commands available by authorization level/functional category

A User Privilege Code also defines the TL1 commands that can be issued to the NE when an NE login is added or modified.

The Functional Categories defined for TL1 commands are:

- ***Maintenance (M)*** - This Functional Category contains all the Fault Management-related features.
- ***Provision (P)*** - This Functional Category contains all the Configuration Management-related features.
- ***Performance Management (PM)*** - This Functional Category contains all the Performance Management-related features.
- ***Security (S)*** - This Functional Category contains all NE Security and Administration-related features.
- ***Test Access (T)*** - This Functional Category contains all the Test Access- related features (applies to Wavestar BWM NEs only).

The Authorization Levels for issuance of TL1 commands are:

- 1 - Minimal (Lowest)
- 2 - Reports Only — merged with Level 1 to be retrieve only
- 3 - General — general provisioning and maintenance functions that are not service-affecting
- 4 - Privileged — privileged user functions that are potentially service-affecting
- 5 - Super User (Highest) — user login specificiation functions

The combination of a Functional Category and Authorization Level consistitues a User Privilege Code (UPC) for a specific set of features. For example, the User Privilege Code “PM3” indicates that a user ID/login is authorized to execute all Performance Management functions with Authorization Level 3 or less. So, the TL1 commands that a user ID/login with this UPC would be authorized to issue are:

- 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 Navis™ Optical EMS is initially set up with pre-defined Command Groups. Each pre-defined Command Group allows issuance of a set of TL1 commands that correspond to certain User Privilege Code levels.

The following is a list of all pre-defined NE Command Groups with User Privilege Codes indicating that level of TL1 commands that can be issued.

Command Group Name	User Privilege Code(s)
Empty	M1,P1,PM1,S1,T1
Maintenance	M4,P3,PM4,S1,T4
Provisioning	M1,P4,PM1,S1,T1
Reports Only	M2,P2,PM2,S2,T2
General	M3,P3,PM3,S3,T3

Privileged	M4,P4,PM4,S4,T4
All	M5,P5,PM5,S5,T5

Refer to the respective network element documentation for an explanation of which TL1 commands can be issued for each Functional Category/Authorization Level.

Related tasks

See the related tasks in Chapter 2, “Security Management”.

□

9 Cluster Administration GUI for Geographically Redundant Navis™ Optical EMS Servers

Overview

Purpose

This chapter provides general information about the cluster administration GUI, which is used to monitor geographically redundant Navis™ Optical EMS servers.

Objectives

This chapter explains how to do the following:

- Identify the different types of host redundancy configurations
- Describe the purpose of the cluster administration GUI
- Use the cluster administration GUI Main window
- Set up user email accounts through the cluster adminstration GUI
- Perform automatic and manual switchovers using the 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 will rely on switching control to another resource on the same host such as a backup LAN card or mirrored disk.
- ***Local Redundancy***—the Navis™ Optical EMS server is supported by a similarly equipped, redundant host located in the same building. Should the primary host fail, the backup host would be 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. Should the primary host fail, the backup host would be activated via manual operation.

Navis™ Optical EMS has a cluster administration GUI that allows an administrator to monitor geographically redundant Navis™ Optical EMSservers in any of the possible high availability configurations. 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 Navis™ Optical EMS server and a geographically remote, redundant Navis™ Optical EMS server can also be set up through the cluster administration GUI.

The cluster adminstion GUI is completely distinct from the regular Navis™ Optical EMS GUI and except for 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 support data replication of the Navis™ Optical EMS database.

The cluster administration GUI supports a 1+1 geographic redudant 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.

Georgraphic failover between the active and standby host can be performed on demand from either:

- The cluster administration GUI
- The command line of the standby server

In order to make the remote station’s server active, the administration GUI can be used to perform a manual 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 EMS application is restarted, a manual switchover must be initiated in order to switch back service to the server.

□

The Cluster Administration GUI

Overview

The Cluster Administation GUI is a simple GUI that monitors the health of the Navis™ Optical EMS servers in the cluster. The GUI main window displays the two georgraphically separated stations, labeled local and remote, with each host contained therein.

Navis™ Optical EMS server icons

Each Navis™ Optical EMS server is represented on the cluster administration GUI by an icon. See Figure 9-1, “Figure 1 - Operational Navis™ Optical EMS Server Icon” (9-4) and Figure 9-2, “Failed Navis™ Optical EMS Server Icon” (9-5).

Figure 9-1 Figure 1 - Operational Navis™ Optical EMS Server Icon

A label just underneath the server icon will display the name of the server and the server’s role in the cluster. The two valid cluster roles are:

Label	Meaning
Active	The associated Navis™ Optical EMS 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 Navis™ Optical EMS 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 Navis™ Optical EMS 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 Figure 9-2, “Failed Navis™ Optical EMS

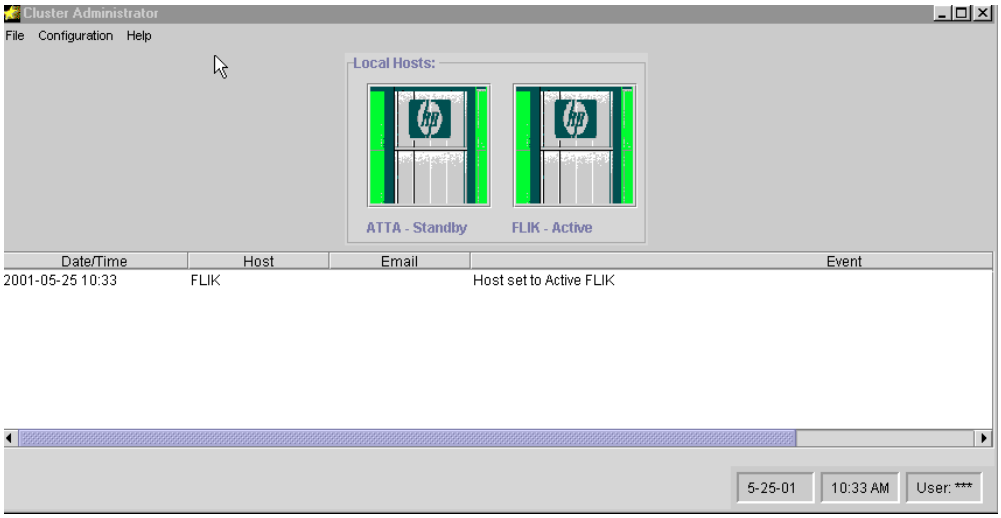
Server Icon" (9-5)). The server is marked as failed until communication is re-established to the server.

Figure 9-2 Failed Navis™ Optical EMS Server Icon

Cluster administration GUI Main Window

Figure 9-3, "Cluster Administration GUI Main Window (1+1 Configuration)" (9-5) shows an example of the cluster administration GUI Main Window Administration window for a 1+1 configuration.

Figure 9-3 Cluster Administration GUI Main Window (1+1 Configuration)



Cluster Administration GUI Features

Email and user configuration

The cluster administration GUI will send email and/or page a set of users when

- any Navis™ Optical EMS 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 Navis™ Optical EMS server may also send email messages when a failure or abnormal condition is detected. In each case, the messages, sent to the user, are hardcoded strings that indicate:

- the reason for the email/page,
- the source of the email/page (in other words, the Navis™ Optical EMS server or the cluster administration GUI)
- the affected Navis™ Optical EMS server

The users, who receive email and/or a page, whether from the Navis™ Optical EMS 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 will be 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 EMSGUI 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 a failure condition is detected by the GUI.

Manual switchover

The cluster administration GUI provides two methods for performing a manual switchover:

- Pressing the Navis™ Optical EMS server icon button on the main window
- Requesting 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 will be 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 Navis™ Optical EMS server. Instead, the `itm` user password is just validated throught the security process of any communicating Navis™ Optical EMS server. If the password is valid, the user is considered authenticated and permission to perform cluster administration GUI operations is granted. However, there is no corresponding server login 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 hand 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, requiring login privilege, is executed. From that point on, the user remains logged in until the user logs out or the cluster administration GUI terminates.

□

10 Trouble Clearing Concepts

Overview

Purpose

This chapter provides reference information to assist in troubleshooting problems with Navis™ Optical EMS and its communications interfaces.

Contents

X.25 Log Files

Overview

The X.25 software on the HP computer maintains a log of any unusual events that may have occurred during the day. These files are located in the */var/opt/acc/log* directory.

Daily X.25 logs

There is one log file for each day of the week.

The files are named as follows:

- *mon.tlog*
- *tue.tlog*
- *wed.tlog*
- *thu.tlog*
- *fri.tlog*
- *sat.tlog*
- *sun.tlog*

Important! Be careful to check the date and time stamp of each file. If today is Friday, but the date and time stamp for the *fri.tlog* file is old, then that file is from a previous Friday and no messages have been logged to the file today. This is very common and indicates there was no unusual activity on the X.25.

X.25 messages

Every X.25 message that appears on the console terminal is also echoed to the appropriate log file.

Here are two of the more common messages that may be found in a log file:

Sample #1:

```
-------------------------------------------------------
Wed Mar 27 14:32:19 1996: zmlog: message logging resumed
-------------------------------------------------------
14:32:19 x25cn 00811 1 Link ZLU 5 DOWN: Link disc. on
   loss of carrier
14:32:35 x25cn 00812   Link ZLU 5 Link established
14:32:35 x25cn 00820   Link ZLU 5 Link restarted
```

The ZCOM Logical Unit (ZLU) Link number is actually the Physical Port Number +1. On the MUX Panel, the ports are labeled J0 through J7 for ports 0 to 7. The ZLU links are numbered 1 to 8, respectively.

Therefore, the above message indicates that Port 4 lost carrier at 14:32:19 on Wed March 27. The link then came back at 14:32:35 and successfully established and restarted Level 2 synchronization.

Sample #2:

```
-------------------------------------------------------
Sat Mar 23 11:55:55 1996: zmlog: message logging resumed
-------------------------------------------------------
11:54:04 zcom  00000   System bootup
11:55:55 zmon  00002   Resource manager (Rev 1.31) for
   ZCOM 4.3.0.0
11:55:55 zmon  00005   Stopping system ...
11:55:55 zmon  00075   ZCOM system stopped
11:55:55 zmon  00002   Resource manager (Rev 1.31) for
   ZCOM 4.3.0.0
11:55:55 zmon  00003   Cold start with: /usr/zcom/cfg/x25.tmem
11:55:56 zmon  00100   Card 0 starting up ...
11:56:04 zmon  00110   Card 0 startup successful, card
   READY
11:56:04 zmon  00020   Cold start completed, ZCOM system
   ready
11:56:04 zmon  00004   Waiting for ZMON requests ...
11:56:04 zcom  00165   Node 123 comes UP
11:56:05 x25cn 00000   X.25 Control Rev 12.2.11p2 - 940303
11:56:05 x25cn 00000   Logical terminal area X25CNT: 88
   Bytes
11:56:05 x25cn 00139   Trace logging disabled
11:56:05 x25cn 00000   COLD start : HGrp# [1-10] : HGrp
   size [1-20]
11:56:05 x25cn 00816   Link ZLU 1 X.25 shutdown complete
11:56:06 x25cn 00811 1 Link ZLU 1 DOWN: Link disc. on
   loss of CTS
11:56:06 x25cn 00816   Link ZLU 2 X.25 shutdown complete
11:56:06 x25cn 00816   Link ZLU 3 X.25 shutdown complete
11:56:06 x25cn 00811 1 Link ZLU 2 DOWN: Link disc. on
   loss of CTS
11:56:06 x25cn 00811 1 Link ZLU 3 DOWN: Link disc. on
   loss of CTS
11:56:06 x25cn 00816   Link ZLU 4 X.25 shutdown complete
11:56:06 x25cn 00816   Link ZLU 5 X.25 shutdown complete
11:56:07 x25cn 00816   Link ZLU 6 X.25 shutdown complete
11:56:07 x25cn 00811 1 Link ZLU 6 DOWN: Link disc. on
   loss of CTS
11:56:07 x25cn 00816   Link ZLU 7 X.25 shutdown complete
```

```
11:56:07 x25cn 00811 1 Link ZLU 7 DOWN: Link disc. on
   loss of CTS
11:56:07 x25cn 00816   Link ZLU 8 X.25 shutdown complete
11:56:08 x25cn 00812   Link ZLU 8 Link established
11:56:08 x25cn 00811 1 Link ZLU 5 DOWN: Link NOT
   established on ENABLE
11:56:10 x25cn 00812   Link ZLU 5 Link established
11:56:10 x25cn 00820   Link ZLU 5 Link restarted
11:56:12 x25cn 00812   Link ZLU 4 Link established
11:56:12 x25cn 00813   Link ZLU 8 reset: Reset due to
   received SABM
11:56:12 x25cn 00820   Link ZLU 4 Link restarted
11:56:15 x25cn 00820   Link ZLU 8 Link restarted
```

The preceding message indicates that the X.25 processes were restarted at 11:54:04 and finished re-establishment of communications at 11:56:15. The software download to the MUX Card was successful. If there was a problem with the MUX Card, it would have been reported here.

The Link ZLU lines at the bottom of the display report which links re-established Level 2 synchronization.

Checking X.25 level 2 status

You can retrieve the Level 2 status by using the `X25_check` command at any time.

Related tasks

See the following related tasks in the Trouble Clearing chapter:

- “Check Level 2 Status of X.25 Network Connections” (6-15)
- “Check the Virtual Channel Status of an X.25 Port” (6-17)
- “Obtain X.25 Virtual Channel Non-Data Packet Statistics” (6-19)
- “Obtain X.25 Virtual Channel Data Counters” (6-20)
- “Reset an X.25 MUX Port” (6-22)
- “Restart X.25 Processes” (6-23)

□

Navis™ Optical EMS/Navis™ Optical NMS Interface Troubleshooting

Overview

There are two Navis™ Optical NMS interfaces supported by Navis™ Optical EMS. The first interface is a server to server interface and the other interface is a GUI to GUI interface.

The server to server interface is responsible for passing NE information from Navis™ Optical EMS to Navis™ Optical NMS. The interface is called the northbound TL1 interface in Navis™ Optical EMS jargon and the southbound interface in NM terminology. The interface takes place over a socket connecting the Navis™ Optical NMS server to the Navis™ Optical EMSserver.

The GUI to GUI cut-through allows Navis™ Optical NMS to invoke the Navis™ Optical EMS GUI screens from the Navis™ Optical NMS GUI. This feature is called the F-interface in both Navis™ Optical NMS and Navis™ Optical EMS terminology. Both GUIs must be installed on an NT Terminal Server and be properly configured to talk to one another. The interface supports a one-to-many configuration where one Navis™ Optical NMS GUI can talk to many Navis™ Optical EMS GUIs of different versions.

Important! If notifications are not received by Navis™ Optical NMS (SONET), verify that the local DNS Domain Name is not set.

GUI-to-GUI interface setup

Configuration File

A configuration file, called *emsFint.cfg*, is delivered with each release of Navis™ Optical EMS. This file will define the operation of the F-interface. The configuration parameters defined by this file are:

1. whether debugging is enabled for the F-interface software
2. the idle-session timeout for the F-interface.
3. mapping of the Navis™ Optical EMS software version number to directories containing Navis™ Optical EMS GUI software on the NT Terminal Server
4. override username and password settings for Navis™ Optical EMS login

The file is a flat, ASCII text file editable by the notepad program. Configuration parameters are defined as name value pairs. Help text in the file explains the purpose of each parameter.

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

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

The file is identical across all versions of Navis™ Optical EMSsoftware.

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

/jui/jnm/itm/southbound/ems/emsFint

Debugging Configuration Parameter

The default debugging parameter configuration file entry is:

debug false

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

When debugging is enabled on the F-interface, the debug output will be captured in the Navis™ Optical NMS output log file.

Idle Timeout Configuration Parameter

The default idle session timeout configuration file entry is:

idleTimeout 600

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

The timeout value is defined in seconds so the default timeout value, as displayed above, is ten minutes. The idle session timeout can be disabled by setting the value to 0.

Release Number/GUI Directory Mappings

When an EMS is defined in the Navis™ Optical NMSdatabase, 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.

Valid release numbers can be any string, but typical values are: R3.0, R2.1. The configuration file must define a directory for each release number defined in 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
release          R6.0 class=itm.southbound.ems.emsfint.EmsFint
```

The first line defines the GUI software that will be used when an undefined release number is found by the F-interface. In this case, when a unknown release number is sent via the F-interface, the GUI contained in the \emsR2 directory will be used.

IMPORTANT: these definitions assume that the Navis™ Optical NMS GUI and the Navis™ Optical EMS GUIs are located on the same drives (generally C drive).

Username and Password Configuration Parameters

By default, the user login name for the F-interface is itm and the password is itm+123. For security reasons, default passwords are not defined in the configuration file. However, if configuration parameter entries are entered in the configuration file, the defined entries will override the default values.

Valid configuration file entries for username and password are:

```
user                    itm password

itm 123
```

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:

EMSDIR=%3\emsR10
EMSPATH=%EMSDIR%;%EMSDIR%\jars\swing.jar;%EMSDIR%\jars\IE.jar;%EMSDIR%\jars\org.jar

CLASSPATH=<NM Classpath>;%EMSPATH%

Navis™ Optical EMS R2.1 and Navis™ Optical NMS R4.2 Cut-through Inter-operability

Due to functionality changes between Navis™ Optical EMS Releases 2.1 and 4.2, the data communicated on the F-interface is different between the two releases of GUI software. Therefore, the data file (i.e. java class file) from the Navis™ Optical EMS R4.2 software must be copied into the emsR2.1 directory.

To copy the file, execute the following command on at the MS_DOS prompt:

```
copy
\emsR3\ems\fint\emsFintObject.class\emsR2.1\ems\fint\emsFintObject.cla
```

In addition, the *\jui\jnm\run_jnm.bat* needs to be changed so that the Navis™ Optical EMS R4.2 replaces the Navis™ Optical EMS R2.1 classpath in the Navis™ Optical NMS startup script: */jui/bin/run_jnm.bat*

Related tasks See the following related tasks in the Trouble Clearing chapter:

- “Test Navis™ Optical EMS to Navis™ Optical NMS Cut-Through” (6-37)

□

Index

Y