User's Guide

EDACS® NETWORK MANAGEMENT

ERICSSON ⦚

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

LIST OF FIGURES AND TABLES

This page intentionally left blank

1. PREFACE

This is one of four manuals for the EDACS® Network Manager. This manual provides operating instructions for users and administrators of the Network Manager system.

Additional documentation for the Network Manager is available in the following publications:

- *EDACS Network Management System Manual* (LBI-39215):
  This manual provides a system level overview of EDACS Network Management.

- *EDACS Network Management Enterprise Management Information Base (MIB) Reference Manual* (LBI-39170):
  This manual contains the EDACS common MIBs and defines each item identified within the MIB groups.

- *EDACS Network Management Installation Manual* (LBI-39171):
  This manual contains detailed information for installing, configuring, and customizing the Network Manager application and the EDACS SNMP Agent platforms.

1.1 MANUAL ORGANIZATION

The manual is divided into the following sections:

Section 1   **Preface** - The preface section identifies the other manuals in the Network Manager manual set and introduces the reader to the organization of this manual.

Section 2   **Documentation** - This section provides a list of Ericsson documents for the associated EDACS elements which might interface with the Network Manager. It also provides a list of manual and documents which may be obtained (or are provided) by vendors and outside sources.

Section 3   **Introduction** - This section provides an overview of the Network Manager, listing its functions and features.

Section 4   **Network Manager Basics** - This section describes some of the basic processes the operator will use when running the Network Manager application.

Section 5   **Startup Procedures** - This section provides step by step procedures for starting and stopping the Network Manager application.

Section 6   **Retrieving Software Version** - This section provides instructions for obtaining the current revision levels of software running on the Network Manager platform and associated devices.

Section 7   **EDACS Help** - This section provides information on using the EDACS Help function.

Section 8   **Monitoring EDACS Fault Conditions** - This section provides instructions for using the Network Manager to detect, isolate, and report alarm or fault conditions associated with the various Network Elements.

Section 9   **Configuring EDACS Devices** - This section provides instruction for running and configuring devices directly connected to the Network Manager, such as CEC/IMC Manager for Windows NT and the System Manager.

Section 10   **Transferring Device Files** - This section information for using the Accounting: File Transfer option, and provides examples on its use.

Section 11   **Monitoring Performance Trends** - This section provides instructions for invoking two-dimensional line graphs, the MultiSite Monitor, and the Site Monitor. This allow the user to evaluate the network's past and present performance and to identify any adverse trends or areas requiring optimization.

Section 12   **Monitoring Real-Time Call Activity** - This section provides instructions for using the MultiSite Monitor and Site Monitor to monitor real-time call activity. The monitors are customizable to meet the user's needs.

Section 13   **Using OpenView Network Node Manager** - This section provides supplemental information on using some of the features available through HP OpenView Network Node Manager.

Section 14   **Procedures** - This section provides procedures for customizing, configuring, and maintaining the Network Manager application.

Section 15   **Troubleshooting** - This section presents a list of problems which may be encountered and possible corrective action.

Section 16   **Glossary** - Contains a glossary of terms.

Section 17   **Index** - This section provides a quick reference to key functions throughout the manual.

2. DOCUMENTATION

In may be necessary to consult one or more of the following documents when operating the Network Management system.

2.1 HEWLETT-PACKARD DOCUMENTATION

The following Hewlett-Packard (HP) manuals provide additional information on the HP products used with the Network Manager:

- HP 9000 Series Owner's Guide

- B1171-90079   HP Visual User Environment User's Guide

- J2316-90001   HP OpenView Network Node Manager User's Guide

- J2316-90000   HP OpenView Windows User's Guide

- J2310-90002   HP OpenView Windows Application Design and Style Guide

- J2311-90001   HP OpenView SNMP Programmer's Guide and Reference

- J2311-90004   HP OpenView SNMP Management Platform Performance and Configuration Guide with HP Network Node Manager Examples for Release 3.3

- J2319-90002   HP OpenView Programmer's Guide

- J2319-90009   HP OpenView Programmer's Reference

- B2355-90037   HP Remote Access Manual

2.2 RELATED ERICSSON PUBLICATIONS

The following Ericsson publications provide additional information on EDACS elements which interface directly or indirectly with Network Management System:

Console Electronics Controller (CEC) and Integrated MultiSite and Console Controller (IMC) Documentation:

LBI-38662   -   EDACS Console Electronics Controller (CEC) and Integrated MultiSite and Console Controller (IMC) Digital Audio Switch

LBI-38939   -   CEC/IMC Customer-Specific System Documentation Overview

LBI-39031   -   EDACS StarGate Controller Digital Audio Switch Maintenance Manual

LBI-39041   -   EDACS CEC/IMC Digital Dispatch DVIU Equipment Maintenance Manual

LBI-39062   -   EDACS C3 Maestro Console System Maintenance Manual

LBI-39100   -   EDACS C3 Maestro Console System with Enhanced Audio Enclosure

LBI-39124   -   EDACS CEC Manager operations Guide, V4.0l

LBI-39224   -   CEC/IMC Manager for Windows NT

System Manager Documentation:

LBI-38703 - EDACS VAX/VMS System Manager Installation, Setup, and Troubleshooting Technical Reference Manual

LBI-38984 - EDACS VAX/VMS System Manager User's Guide

AE/LZT 123 1908/1 - Keyboard Mapping Template.

Billing Correlation Unit (BCU) and Centralized Activity Logger (CAL) Documentation:

LBI-38965 - EDACS BCU/CAL System and Installation Manual

LBI-38967 - EDACS Billing Correlation Unit/Centralized Activity Logger (BCU/CAL) User Interface Manual

Data Gateway Documentation:

LBI-38961 - EDACS Data Gateway Technical Description

LBI-38962 - EDACS Data Gateway Installation and Maintenance Manual

LBI-38963 - EDACS Data Gateway User's Reference Manual

LBI-38964 - EDACS Data Gateway Configuration Reference Manual

Jessica PBX Gateway Documentation:

LBI-39000 - EDACS Jessica PBX Gateway Systems Manual

LBI-39001 - EDACS Jessica PBX Gateway Operator's Manual

LBI-39039 - EDACS Jessica PBX Gateway MD110 Configuration Manual

LBI-39040 - EDACS Jessica PBX Gateway PI User's Manual

LBI-39080 - EDACS Jessica PBX Gateway Operator's Manual (Pocket Guide)

Miscellaneous Ericsson Documents:

ECR-1895 - Glossary of Mobile Radio Terms including Acronyms and Abbreviations.

Protocol Standards:

rfc-1213 - Management Information Base for Network Management of TCP/IP-Based internets: MIB-II.

3. INTRODUCTION

The International Organization for Standards (ISO) Network Management forum identifies five functional areas of network management, often referred to simply as "FCAPS." This model serves as the basis for the Network Management system. The five management areas are as follows:

- **F**ault Management

- **C**onfiguration Management

- **A**ccounting Management

- **P**erformance Management

- **S**ecurity Management

In addition to the functional areas listed above, the EDACS Network Manager also provides the following:

Integrated CEC/IMC Manager	Using an integrated client on the EDACS Network Manager platform, administrators can view the same data, using the same windows that are available to technicians who configure and debug locally. In this mode, the CEC/IMC Manager acts as the server, while the application on the EDACS Network Manager participates as a client. The EDACS Network Manager and CEC/IMC Manager platforms provide a client-server applications that have a common look and feel.
Integration with Other OpenView Network Management Applications	The customer is responsible for maintaining the configuration of the other Network Management applications. The EDACS Network Element icons may exist on the same map as the customer's OpenView T1/Microwave/PBX network icons to form an integrated network management map.
Scaleable Network Manager Platform	The EDACS Network Manager application is available on a variety of HP workstations/servers so that large and small networks can be supported cost effectively.
Multiple EDACS Network Manager Sessions	The EDACS Network Manager allows multiple simultaneous users to be logged in and viewing network information via X-sessions, either from X Stations or PCs running X-terminal emulation.
Internationalization	The EDACS Network Manager Application uses the UNIX Native Language Support (NLS). This feature supports other languages without recompiling the application. Currently, English is the only language supported.
Alarm Log/Reports	A report can be generated listing the past and present alarms.
Basic Help Menu	On-line help for the EDACS Network Manager application.
Internationalization	This feature supports other languages without recompiling the application. Currently, English is the only language supported.

3.1 FAULT MANAGEMENT

Fault Management is responsible for detecting, isolating, and reporting anomalous conditions affecting network operation. Central to the concept of a fault is the fact that some corrective action must be taken, whether automatically over a Local Area Network (LAN) or by manual intervention by technicians at a site.

The following features are available through Fault Management:

Fault Notification	EDACS platforms send all alarm and status event information to a central point. The Network Manager can periodically poll remote devices for missed events. Events are logged at the EDACS Network Manager and displayed on the Hierarchical map. Popup messages or automatic notification actions, such as email, are customizable.
Hierarchical Network Map for Fault Notification	Each Network Management Station is provided a consistent, integrated view of the alarm status of its entire EDACS network. Alarms are propagated from lower network layers all the way up to the top-level map.
Alarm Help	On-line help is provided describing the fault and, where possible, suggesting the corrective action. In addition, to the EDACS-provided alarm information, site-specific alarm help/corrective action suggestions are customizable.
Alarm Log/Reports	A report can be generated listing the past and present alarms.

3.2 CONFIGURATION MANAGEMENT

Configuration Management is responsible for identifying and controlling the state of elements within the network, including subscriber access to the services provided by the network. This management area performs the following:

- Using a local client Graphical User Interface to configure a device.

- Using a Telnet session to configure devices in their native format.

- Reboot, Restart, or Shutdown certain EDACS devices.

Configuration control of the CEC/IMC is through the CEC/IMC Manager for Windows NT. The CEC/IMC Manager for Windows NT employs the client-server paradigm. The server, which interfaces to the CEC/IMC, runs on the Windows NT platform while the client may run on either the Windows NT platform or the EDACS Network Manager UNIX platform. This allows the CEC/IMC Manager user interface to be run either on the EDACS Network Manager or on the CEC/IMC Manager PC.

Configuration Management of other devices is via native access i.e., Telnet session into the System Manager, BCU/CAL, and PI. Each device retains its password protection, therefore users must have login privileges. The ability to log in to multiple platforms and operate in their native modes from one terminal provides a migration path for devices converting to the client-server paradigm.

Remote ability to perform shutdown, restart, and reboot operations to selected EDACS devices is provided. The execution of these actions is recorded in the same log used for alarms.

3.3 ACCOUNTING MANAGEMENT

Accounting Management is responsible for capturing the usage of network resources by end users.

Billing subsystems are available on the BCU (stand-alone), BCU option on the PI platform, and Enhanced Local Interconnect (ELI). Only the BCU and PI are accessible from the EDACS Network Manager (via File Transfer Protocol) to retrieve billing records.

3.4 PERFORMANCE MANAGEMENT

Performance Management is responsible for characterizing the usage and efficiency of the network. This area is conceptually composed of three major areas:

- **Utilization** -- Provides information regarding which aspects of, and the degree to which, the network interfaces are being used.

- **Accessibility** -- Provides information which may be used in determining that the network services are meeting customer expectations.

- **Tuning** -- Provides information which may be used to evaluate adjustments to the network to increase utilization and accessibility.

EDACS devices provide various performance values via SNMP Management Information Bases (MIBs). The EDACS NM requests and receives these values for display and/or collection. The performance values required, and the network element(s) responsible for providing them, are given in the following subsections on a per map object basis.

Graphs to address Utilization and Accessibility may be invoked via menu items. See Section 0. Other parameters may be useful when troubleshooting.

Graphical Performance Monitoring	EDACS Network Administrators can monitor system performance at node and site levels. Results may be saved to disk and later displayed. Performance graphs may also be saved. Performance graphs are available with the Billing Correlation Unit/Centralized Activity Logger (BCU/CAL) or as a separate Jessica Private Branch Exchange Interface (PI) option.
Multisite Monitor	The Multisite Monitor oversees call activity for an entire node. It is available with BCU/CAL or as a separate PI option.
Site Monitor	The Site Monitor oversees call activity for an individual site. It is available with BCU/CAL or as a separate PI option.

3.5 SECURITY MANAGEMENT

The Network Manager provides security of both user and system access. There are three levels of users authorized to use the Network Manager system. These are classified as Administrator (or SuperUser), Technician, and User.

System Access is controlled by assigning user account passwords, assigning unique community names to devices, and through the profile configuration of remote elements.

3.5.1 Access Levels

The classifications of Network Management users are:

- **Administrator** - The Administrator has a full menu set and write access to OpenView, thus complete control over the Network Management system. This allows the administrator to retrieve, view, and change Network Management system attributes. However, only one write copy of OpenView may be operating at any one time. All other simultaneous sessions will be read only.

- **Technician** - The Technician has a full menu set and read only access to OpenView. This allows the Technican to retrieve and view network data, but restricts the Technician from making unauthorized changes to the Network Management system attributes.

- **User** - The User has a reduced menu set and read only access to OpenView. This limits the users access to critical EDACS functions and editing features in OpenView.

3.5.2 System Access

Security Management is responsible for administering user access to network resources, including the Network Elements (NEs) themselves. The approach will encompass:

- Password Protection: Native Access Mode -- Native access refers to currently existing security measures, such as account-password validation. This mode applies to local (i.e., user console) and remote (i.e., Telnet and File Transfer Protocol) access procedures implemented by Network Elements.

- SNMPv1 protocol protection: SNMP provides some inherent security mechanisms. This will mainly serve as protection against data corruption due to application errors.

- To enhance SNMPv1 security, the directly connected NE supports a community name profile which allows restriction of IP Addresses to specific community names with specific read-write access.

3.6 HIERARCHICAL MAPS

The Network Management graphically illustrates an EDACS network by using a set of hierarchical map levels. By traversing down the maps, a greater level of detail is revealed.

Four network levels are suggested:

- EDACS
- Multi-Node
- Node
- Site

All submaps are created such that the icons may be moved freely about the map, there are no restrictions regarding placement of EDACS icons on maps. Thus, all icons could be on one submap if desired. For customers without all the network levels listed above, the EDACS icon will explode into the first available level. The EDACS, Node, and Site icons are explodable icons, meaning that double-clicking on them will bring up the next lower level. See the examples of the Map Traversal Screens shown in Figures 2 and 3.

The EDACS Map Generation Application assists in setting up EDACS maps and is described in the Installation manual, LBI-39171.

A new term "Switching Center" is being introduced with the Network Manager. To represent 30 consoles, 32 sites, BCU/CAL, CEC/IMC Manager, System Manager, EDG, and PI on one map would make the map very busy. Therefore, the term "Switching Center" was coined to represent the devices physically located at the IMC Node.   This includes the IMC, consoles, BCU/CAL, EDG, PI, CEC/IMC Manager, and System Manager. As an analogy to this, the Site represents the devices physically located at the site such as channels, TU, ACU, SC, PMU, and ELI.

All EDACS "symbols" will require identifiers to uniquely identify them. These identifiers are specified in the "EDACS Identifiers" attribute section of the Describe/Modify popup window.

The following is a summary of map features:

Assisted Map Generation	When the following symbols are added, popup windows prompt for information to generate the map hierarchy: IMC Node, CEC Node, Remote CEC Node, Switching Center, and Site.
Customized Maps	As the EDACS NM application leverages HP OpenView Network Node Manager, EDACS icons can be positioned anywhere on the submap. Although Map Generation places icons on default submaps, the customer may create his own hierarchical view. Icons for non-EDACS devices may be placed on EDACS maps.

Background Network Map Overlays	This standard HP OpenView Network Node Manager feature allows customers to flexibly place network icons on top of actual area maps. Topological maps (in standard GIF format) are easily added, but are not provided.
Customizable Icons	The labels on icons may be modified. The user may add text to an icon's object for customer-specific information such as the site contact, location, etc.

3.7 EDACS NM MENUS AND THEIR FUNCTIONALITY

There is a common set of pull-down menu options available to icons. Menu options are grayed out for functions that are not applicable for a specific icon. The EDACS Network Manager's EDACS-specific functionality can only be activated by:

1) Selecting an icon that represents an EDACS manageable element, and

2) Activating the EDACS menu located on the Main Menu bar at the top of the screen.

If an icon is not selected, the EDACS menu option may be grayed out, meaning that it is inaccessible. Figure 1 shows the initial set of submenus which include Faults, Configuration, Accounting File Transfer, Performance, and Software Version. Refer to the following text for additional details on each EDACS menu option.

Faults. Provides alarm information about the EDACS device represented by the icon.

Configuration. Presents configuration functions associated with the EDACS device represented by the icon.

Software Version. Displays the software version information for each directly connected device and its subcomponents.

Accounting: File Transfer. Allows device-specific accounting records or configuration files to be transferred to the EDACS Network Manager using File Transfer Protocol (FTP).

Performance. Presents performance information about the EDACS device represented by the icon.

File...   EDACS   Help

Faults ▷
Configuration ▷
Accounting: File Transfer
Performance ▷
Software Version

Figure 1 - EDACS Menu on Main Menu Bar

4. NETWORK MANAGER BASICS

4.1 PULLDOWN MENU SELECTION PROCEDURE USING THE MOUSE

Select <u>one</u> of the two options below to select the Pulldown Menu:

Position the cursor to the desired menu option, and quickly press/release the left mouse button once. The pulldown menu will fix itself to the screen. Position the cursor to the next desired option, and press/release the left mouse button once.

OR

Position the cursor to the desired menu option, press (but do not release) the left mouse button. Drag the cursor to the next desired option and release the left mouse button.

4.2 PULLDOWN MENU SELECTION PROCEDURE USING THE KEYBOARD

Each menu option contains a mnemonic (one-letter hot key) that is shown visually with an underline. To select an option on the main menu bar, press the ALT key and the mnemonic simultaneously. A pulldown menu will appear. Press the mnemonic of the next desired option to select it.

4.3 EDITOR OPTIONS

vuepad editor - HP VUE editor, menu-driven, simple, intuitive

> **> /usr/vue/bin/vuepad filename**

NOTE: Also available via an icon on the VUE menu pad. Automatically invoked via the File Manager utility when the user chooses to edit a file.

NOTE: To edit a file, the file must have write privileges for your user type. See the Unix man pages for the chmod / chown commands to reset file permissions and ownership.

vi editor - standard Unix editor, command-driven

> **> vi filename**

NOTE: Recommend book by O'Reilly & Associates, Inc. entitled ***Learning the vi Editor***

4.4 MAP TRAVERSAL

The following submaps are examples of map traversal. The first two submaps contain background graphics, while the last two do not. Background graphics may be loaded in all submaps.

Exploding the EDACS   icon brings up a screen similar to that shown below.
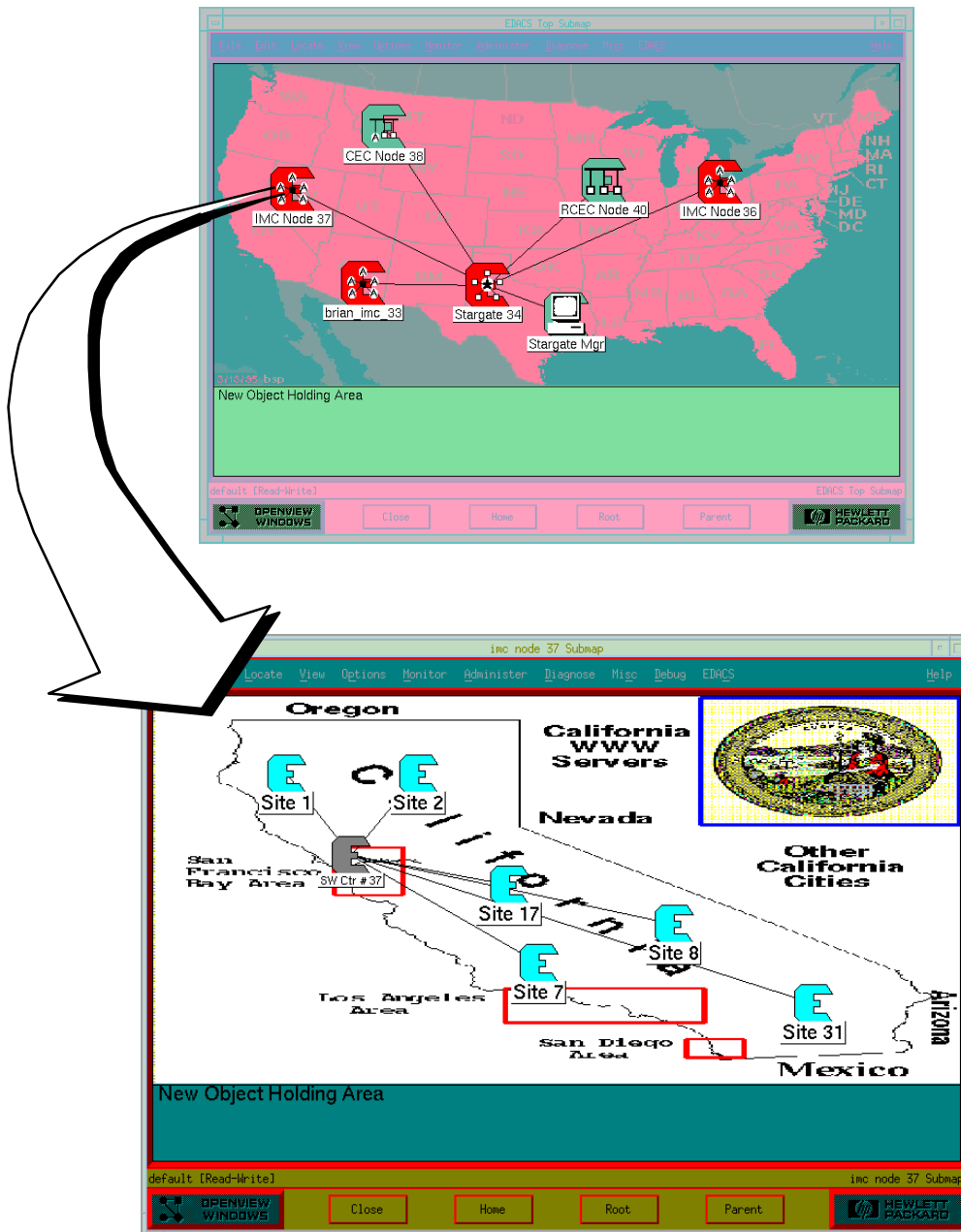
Exploding the IMC Node 37 icon brings up the IMC Node 37 submap screen similar to the one shown above.

Figure 2 - Example of Map Traversal

Exploding the Switching Center icon (SW Ctr #37) on the IMC Node 37 submap brings up a Switch Center 37 submap similar to the screen shown below.
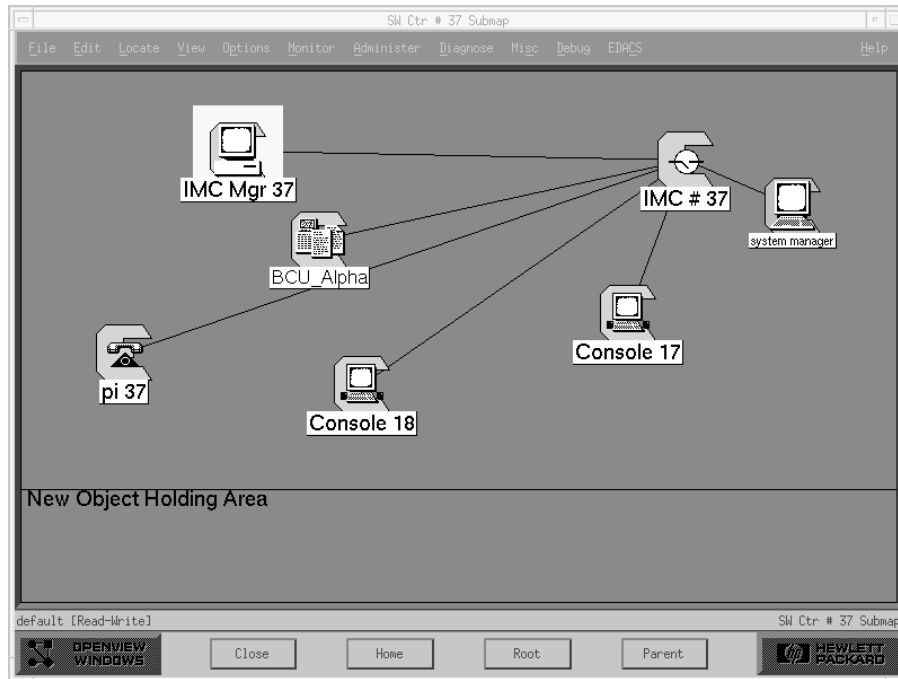
Exploding a Site icon (such as Site 1) on the IMC Node 37 submap brings up the Site 1 submap similar to the screen shown below.
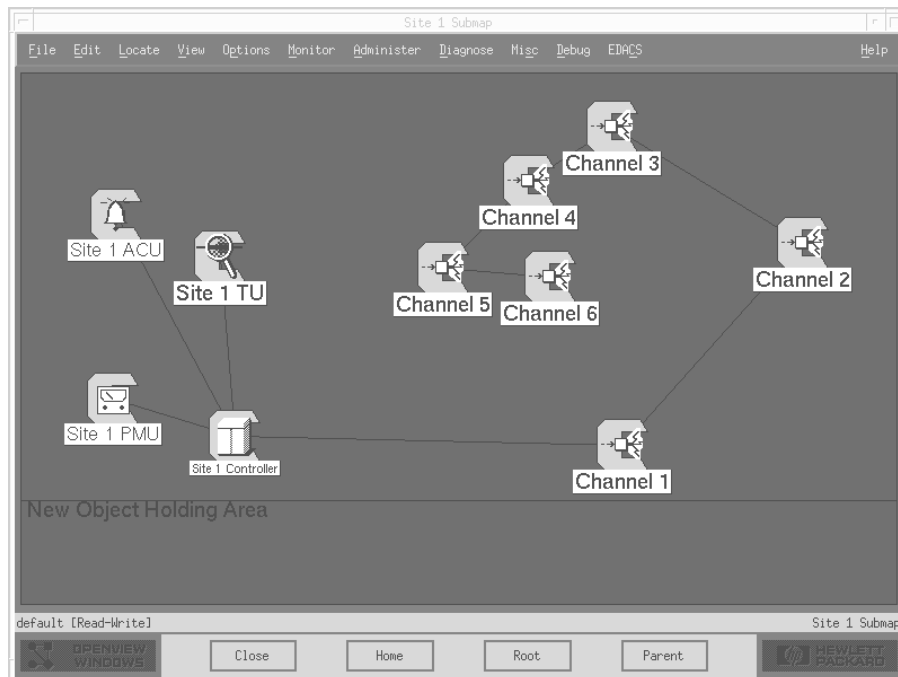
Figure 3 - Example of Exploding a Switching Center and Site Icon

5. STARTUP PROCEDURES

Use the following procedures to login and start a Network Manager work session. A Network Manager work session is described as the time between logging in and logging out.

5.1 STARTING A NETWORK MANAGER WORK SESSION

The Ericsson Login Screen is the gateway to the Network Management System. After entering your login name and password, the session will start by displaying HP VUE (Visual User Environment) screen containing the HP VUE Front Panel.

Login into the Network Management system by using the following procedures:

1. Select the Login box and enter your login name. Press the *<ENTER>* button or use the mouse and place the cursor in the Password box.

2. Type in your password. Press the *<ENTER>* button or click on **OK**.

    If the Login Manager does not recognize your name or password, click on **CLEAR** and reenter the information.

3. Successfully logging into the HP OpenView session will result in displaying the HP VUE Front Panel.
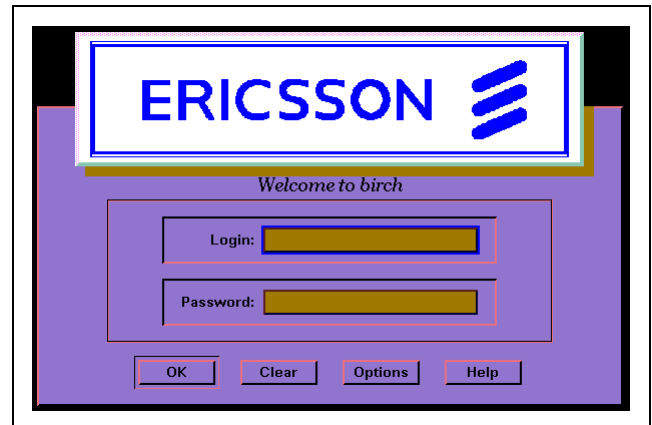
Figure 4 - Network Manager Login Dialog Box
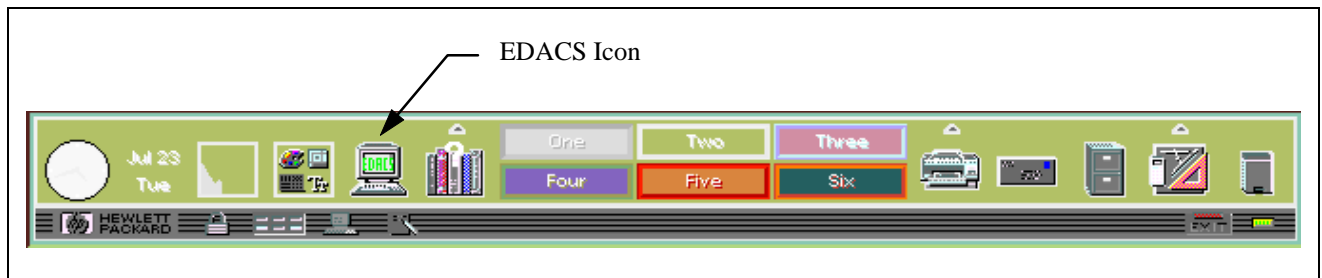
Figure 5 - Network Manager Login Dialog Box

4. Start the Network Manager application by clicking on the EDACS icon. The terminal will display a READ version Network Management Home submap.

    Additionally, a popup message will be displayed indicating the Polling Status and the Clock Synchronization Source.

5. You are now able of retrieve and view those Network Management attributes authorized by your Network Administrator.

5.2 ENDING A NETWORK MANAGER WORK SESSION

Use the following procedures to properly end a work session.

CAUTION

When you finish a working session, <u>DO NOT</u> turn off the Network Manager Station. This equipment is part of a multi-user network, and other people may be using it. If you turn off the Network Manager station, you will deny them access to it.

NOTE

If a complete system shutdown is required, refer to the System Shutdown Procedures after logging out.

5.2.1 LOGGING OUT OF THE NETWORK MANAGER SESSION

To exit the Network Management session, perform the following:

1. From any Network Management submap, select File->Exit from the menu bar.

2. OpenView will display a Warning popup menu, indicating your session is ending. Click on OK to end the session.

3. OpenView will close all applicable files and return to the HP VUE screen.

5.2.2 LOGGING OUT OF THE HP VUE SESSION

To completely exit the HP VUE session, perform the following:

1. Click on the EXIT button on the HP VUE Front Panel.

2. The Session Manager will prompt you with the Logout Confirmation popup menu.

    This popup menu will indicate "This session not saved. Instead your Home Session will be restored upon startup." This is normal operation configured into the system during installation. If it is necessary to make changes to the Startup Session, consult with your Network Administrator.

3. Click OK to continue the logout process.

4. After logging out, the terminal will return to the Login screen.

6. RETRIEVING THE SOFTWARE VERSION

The Software Version feature allows you to obtain the versions of software installed on the Network Manager platform and software installed on directly connected devices and the devices they proxy for.

6.1 SUBCOMPONENT SOFTWARE VERSIONS

All software versions for the directly connected device and its subcomponents are available by using the following procedure:

1. From the hierarchical map, select the icon representing the desired subcomponents.

   NOTE: If an icon is not selected, the EDACS->Software Version menu may be greyed out.

2. The Network Manager will respond with the Software Table screen showing the software versions of all devices (or boards) directly connected to the selected device.

   For example, the response to an inquiry about the software version of the CEC/IMC Manager includes the versions of its boards as shown in Figure 6. The IP Address or host name of the directly connected EDACS device is listed in the IP Address field.

3. Select the CLOSE button at the bottom of the screen to exit the Software Table screen.
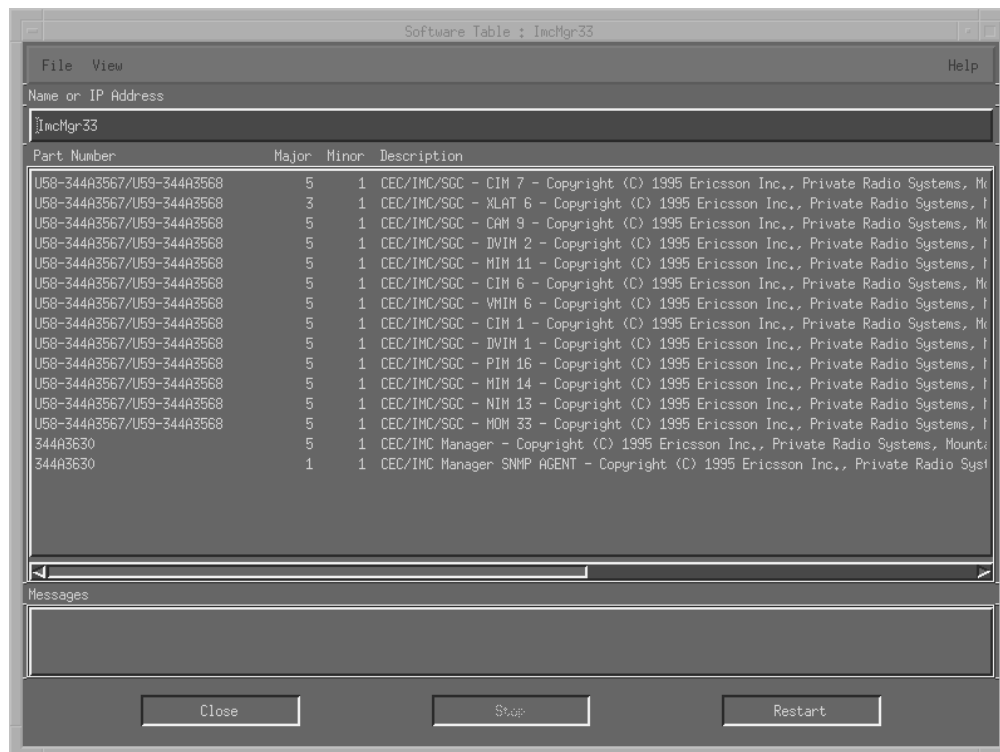
Figure 6 - Software Version Screen Example

Part Number   The Part Number field identifies the Ericsson Part Number of the software. If the software is installed on a ROM chip, then the part number will be preceded by the ROM's reference designator (or location).

Major Version   The Major Software vision is an integer number representing the major software revision number, for example the number "2" in 2.1.

Major Version   The Minor Software vision is an integer number representing the minor software revision number, for example the number "1" in 2.1.

Description   The description field provides a brief description of the software component.

Software Path   This field will identify the ROM or the location of the software on the disk.

6.2 NETWORK MANAGER SOFTWARE APPLICATION VERSIONS

A list of software applications installed in the Network Manager and their software version can be obtained by using the following procedure:

1.   Select Help -> On <u>V</u>ersion from the Main Menu Bar.

2.   The Network Manager will display a list of software installed in the Network Manager and their software versions.

A list of software applications, their software version, copyright data, and description can be obtained by using the following procedure:

1.   Select Help -> Index -> Application from the Main Menu Bar.

2.   The display will list the application software installed in the Network Manager platform.

3.   Select the desired application and the pertinent data will be displayed.

7. EDACS HELP

EDACS Help has been integrated into the OpenView Network Node Manager help system. EDACS Help items are preceded with "EDACS" to make them easily identifiable.
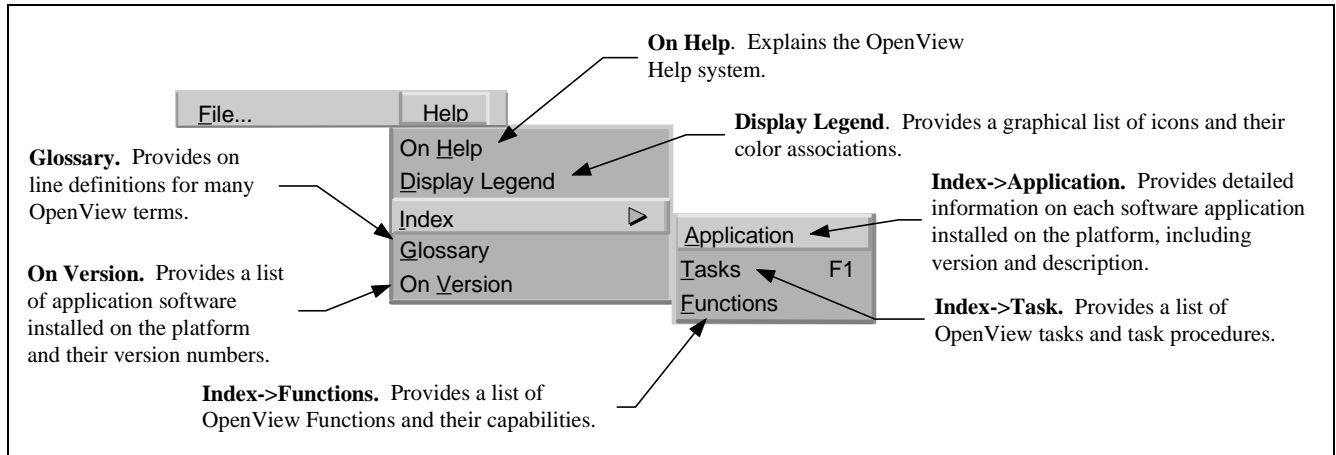
Figure 7 - EDACS Help Menu

7.1 TASK HELP

On-line help is available for performing various EDACS and OpenView tasks. The Task Index provides a list of OpenView and EDACS menu bar and Map Generation help files and when opened, provides detailed procedures for performing the task. Perform the following when requesting task assistance.

1. Select Help -> Index -> Tasks from the Main Menu Bar.

2. The display will list the various OpenView and EDACS tasks.

3. Select the desired task and the click on the Open button.

4. OpenView will provide a description of the task and suggested procedure.

7.2 FUNCTION HELP

On-line help is available for performing various OpenView functions. The Function Index provides a list of OpenView and EDACS Functions and when opened, provides detailed procedures to perform the function. Perform the following when requesting on assistance.

1. Select Help -> Index -> Function from the Main Menu Bar.

2. The display will list the various OpenView functions.

3. Select the desired function and the click on the Open button.

4. OpenView will provide a description of the function and recommended usage.

8. MONITORING EDACS FAULT CONDITIONS

Fault Management is responsible for detecting, isolating, and reporting alarm or fault conditions affecting the various Managed Elements (ME) in the EDACS network.

8.1 DETECTING AND ISOLATING FAULTS (ALARMS)

Fault (alarm) or event status notification results from the Network Manager either receiving information from the EDACS platforms or as a response to polling. When an event is received the user is notified of the event through the Event Notification Interface or by changing the color of the appropriate icon on the hierarchical maps.

EDACS Fault Management tracks five user-configurable severity levels for each managed EDACS Network Element:

- **Normal**   An application sets the status to "normal" when the object is in a normal operational state.

- **Warning**   An application sets the status to "warning" when an object may face a potential problem.

- **Minor**   An application sets the status to "minor/marginal" when an object has a minor problem; this status should not, however, impede the normal use of the device.

- **Major**   An application sets the status to "major" when an object has serious problems; these problems are likely to impede normal use of the device.

- **Critical**   An application sets the status to "critical" when a device is not functioning or is not accessible by the EDACS Network Manager.

Table 1 lists the severity levels, descriptions, and associated colors. The severity levels and colors are configured according to HP OpenView Network Node Manager conventions. Each alarm received is tracked internally. The color of the icon does not change until all alarms received at that severity level have cleared, or an alarm at a higher severity level is received. For the EDACS Network Manager application, green icons indicate there are no known managed faults against the device represented by the icon.

Fault Management can periodically poll remote elements for missed traps. Elements on unlicensed nodes or sites will have Restricted status, and any corresponding traps will be ignored. Refer to *FCAPS* section in LBI-39215 for the actual fault items and Table 1 for the meaning of icon colors. The meaning of icon colors may also be obtained by selecting the Help -> Display Legend from the main menu.

8.1.1 Notification through the Event Notification Interface

Once an alarm is generated, it is logged into the Event Logs. After the event is logged, the alarm specifics are available through the Event Notification Interface. The Event Notification Interface includes the Event Categories window and the multiple Event Browser windows.

The Event Categories Window acts as an event notification window. The push buttons in this window light up to indicate when events have been received and have not been deleted from the Events Browser. The color of the push button reflects the most severe event in the category, or background color if no events are present. The "All Events" category contains all the events which are present in the other categories. The "EDACS Events" category is added by the Network Manager application software.

8.1.2 Notification Through Icon Color

After the Network Manager logs the event, it will change the appropriate map icon(s) color if necessary, and if enabled, display a popup window reporting the event and its severity.
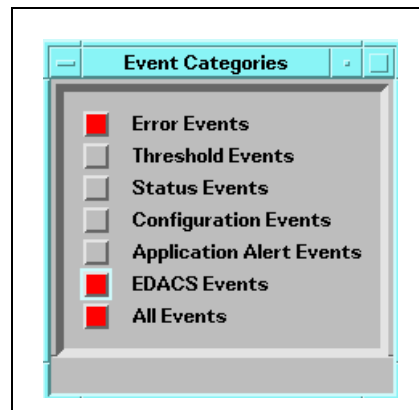
Figure 8 - Event Category Window

Table 1 - Status Colors/Levels

Category	Status Condition	Status Meaning	Icon Color
Administrative	Unmanaged	Users can set this value, which indicates that the object should not be monitored and that the status should be ignored. When the user sets the object back to "managed." the EDACS->Fault->Update operation must be performed.	Off-white
Administrative	Testing	An application sets the status to "testing" when an object is undergoing temporary diagnostic or maintenance procedures. This category is not used by the EDACS Network Manager application.	Salmon
Administrative	Restricted	An application sets the status to "restricted" when a valid associated CEC/IMC/RCEC/SG node license does not exist for this element.	Tan
Administrative	Shutdown	An application sets the status to "shutdown" when an object is inactive (although there may not be anything necessarily wrong with the object). This category is not used by the EDACS Network Manager application.	Dark Brown
Operational	Unknown	An application sets the status to "unknown" when the status of an object cannot be determined. EDACS icon may be blue if there is another icon with the same Network Number and Node Number or if polling does not detect a physical device corresponding to this icon.	Blue
Operational	Normal	An application sets the status to "normal" when the object is in a normal operational state.	Green
Operational	Warning	An application sets the status to "warning" when an object may face a potential problem.	Cyan
Operational	Minor/ Marginal	An application sets the status to "minor/marginal" when an object has a minor problem; this status should not, however, impede the normal operation of the network.	Yellow
Operational	Major	An application sets the status to "major" when an object has serious problems; these problems are likely to impede normal use of the network.	Orange
Operational	Critical	An application sets the status to "critical" when a device is not functioning or is not accessible by the EDACS Network Manager.	Red

The user is able to determine the Managed Element's operating condition at a glance by observing the icon's color. Upon receiving an alarm, the event is logged and the icon color is changed to the color representing the severity of the alarm. To ensure alarms are not missed, the fault color propagates up to the top-level icon on the root map. The top level icon will always reflect the color of the most severe fault propagated up from its submaps.

An EDACS Icon is managed if it has one of the following states: restricted, normal or alarm. The OpenView Help->Display Legend gives the association of state to color. An icon will be brown (indicating restricted) unless it has an associated licensed IMC/CEC/RCEC/StarGate icon with the same EDACS Identifiers (Network Number and Node Number).

An EDACS icon will be blue if all of the elements on its submaps are restricted or unmanaged. An EDACS icon will also be blue if there is another icon with the same EDACS identifiers. The last one added with those EDACS identifiers will be managed.

An icon may be red if it is inaccessible from this Network Manager station. The EDACS->Fault->Summary menu item will give a descriptive message regarding the state of the remote element.

The Network Manager application counts the number of unique outstanding alarms at each severity level: Critical, Major, Minor, Warning, and Normal. The icon color should be the same as the highest severity level and should not change until all alarms at that severity level have cleared. When all alarms at the highest severity level have changed, the icon color should change to the next lowest severity level.

8.1.3 Fault Propagation

If there are no outstanding alarms, the icon color should correspond to the normal level. Icon color will propagate up the hierarchical levels. There are options to propagate the most critical or the average alarm level. Select EDIT->Describe/Modify Map and set Map to Propagate Most Critical.

8.2 REPORTING FAULTS (ALARMS)

OpenView Network Node Manager provides choices for alarm propagation. The parent icon may be configured to reflect the highest alarm state, an average alarm state, or a threshold.

8.2.1 Fault Configuration

The **EDACS->Faults->Configuration** menu item generates the OpenView Network Node Manager Event Configuration dialog box with an associated help button. This feature allows actions and popup windows to be associated with events, modifications of the category, and severity level. However, it does not allow configuring the threshold-oriented alarms. When configuring threshold-oriented traps at the Network Manager station, refer to the Options -> Data Collection menu item. When configuring Threshold-oriented traps at a remote element, use the procedures in the section titled *Setting Threshold Traps On Collected Data*.

The action(s) to be performed following the receipt of an alarm is user-selectable on a per alarm basis. Multiple actions may be selected simultaneously. The list of possible actions is shown below.

- Log the event with an entry describing the alarm, time of occurrence, source, and severity.

- Display a popup window describing the alarm, time of occurrence, source, and severity.

- Output to a printer describing the alarm, time of occurrence, source, and severity.

- Execute a user-defined application resident on the EDACS NM or another network device via a remote procedure call. This can include such tasks as issuing a data message to an EDACS data terminal, sending an e-mail message, calling a pager, or making a telephone call.

- Produce an audible beep.

The EDACS NM application provides a default alarm definition, description, severity level, and category. The alarm definition and descriptions can be restored to their default values by executing **/usr/OV/bin/xnmevents -load**

/usr/EDACS/conf/C/ed_trapd.conf. The severity levels and category will not be restored and will remain as customized by the user. The restore operation will not erase the actions which have been associated with individual alarms.

NOTE

Modifications to severity level will be made to all devices with that alarm. If the alarm is currently active, the icon will reflect the severity level change.

8.2.2 Latching Transient Events

If faults are setting and clearing is a short time frame, they may not be visually obvious. Of course the events would be listed in the Event History. A popup message may be associated with any event to capture the transient nature. Link failures that come and go are candidates for this action.

To associate a popup message with a particular event one may either invoke the **EDACS->Fault Configuration** menu item, which requires the user to locate the event under the enterprise agent providing the event, or select the event in the event browser and select the event browser **Actions->Event Configuration**, which points the user to the event the user wishes to add the popup to. Either procedure will bring up the Event Configuration window.

NOTE: If the event has the concept of setting and clearing, like a link failure, then the popup will occur on both the setting and clearing event.

8.2.3 Associating Actions With Events

Any command executable from the UNIX command prompt may be associated with an event including a email message or a beep.

To associate an action with a particular event one may either invoke the **EDACS->Fault Configuration** menu item, which requires the user to locate the event under the enterprise agent providing the event, or highlight the event in the event browser and select the Event Browser **Actions->Event Configuration**, which points the user to the event the user wishes to add the action to.

NOTE: If the event has the concept of setting and clearing, like a link failure, then the popup will occur on both the setting and clearing event.

8.2.4 Disabling Events at Remote Agent Devices

Erroneous events, which may be caused by broken hardware, may be disabled at the remote platform. In general, each event with the concept of setting and clearing may be individually disabled at the remote platform. Note: this disables the event number. For example, if the SM_Site_Link event is disabled at the System Manager, than all SM_Site_Link events are disabled even if only one site link is a problem.

Figure 9 - Event Configuration

You may not individually enable/disable events reported by the IMC Manager. However, it does support a enable/disable <u>all</u>. Refer to the System Manual, LBI-39215, for a listing of Events and the MIB Objects used to disable them.

8.2.5 UnManaging Devices

If a device is undergoing maintenance, it may be desirable to unmanage its associated icon to prevent its state from propagating up the map levels.

To unmanage a device, perform the following:

1. Select the icon.

2. Select the **Options->Unmanage Object** menu item.

3. Verify that the device's icon color turns off-white. This indicates that the status of the device is is being ignored.

8.2.6 Managing Devices

To manage a device which was previously designated as Unmanaged, perform the following:

1. Select the icon.

2. Select the **Options->Manage Object** menu item.

3. Verify that the device's icon color turns blue. This indicates that the device is being monitored, but its current status has not been updated and is unknown. To determine the device's current status, perform the Fault Update procedure.

8.2.7 Fault Updating Managed Devices

This menu item allows you to manually update EDACS managed icons with the latest status reported to the EDACS Network Manager. When an icon transitions from unmanaged to managed, this menu item must be used to update the menu items.

Use the following procedure to update the status of a managed device:

1. Select the icon representing the device.

2. Select the **EDACS->Fault->Update** menu item to manually update the device's current status.

3. The device's icon will change to the color corresponding to last status reported to the Network Manager.

8.2.8 Setting-up Threshold Oriented Events at RTM Devices

The BCU/CAL and PI devices are threshold-oriented alarming mechanisms. This thresholding allows the configuring of such parameters as rising or falling trap and the conditions for generating traps. The OpenView MIB Browser is used to configure these traps. For additional informatio, refer to the section on Setting and delecting alarm thresholds in LBI-39171.

8.3 IDENTIFYING THE CAUSE OF ALARMS

8.3.1 Using Hierarchical Maps

After the Network Manager alerts the user to an alarm either by changing an icons color or through a popup window, it will be necessary to identify the responsible element causing the fault indication and isolate the cause.

The hierarchical maps display a greater level of detail as the maps are traversed. To prevent missing fault status, fault colors propagate to the top level icon on the root map. The easiest method of identifying the element causing the fault is to traverse down the maps until the element in question is displayed.

Events can be one shot or possess the concept of setting and clearing. Only events possessing the concept of setting and clearing, such as linkup/down or board fail/normal, change icon color. For a given map object, the Network Manager can display the current alarms affecting icon color for that object.

1. Traverse down the hierarchical maps by double-clicking with the left mouse button on the faulted icon. This will open any submap associated with the icon.

2. Continue traversing down through the submaps until the managed element causing the alarm has been identified.

3. Select (highlight) the icon with the fault color using the left mouse button.

4. Select the **EDACS -> Faults -> Summary** menu item.

The summary popup window listing all known actively managed faults received asychronously or detected by EDACS

Double click on faulted icon to traverse to next lower level.

Highlight faulted icon, and select the EDACS->Faults->Summary to view the Alarm Summary for the icon selected.

Alarm Summary
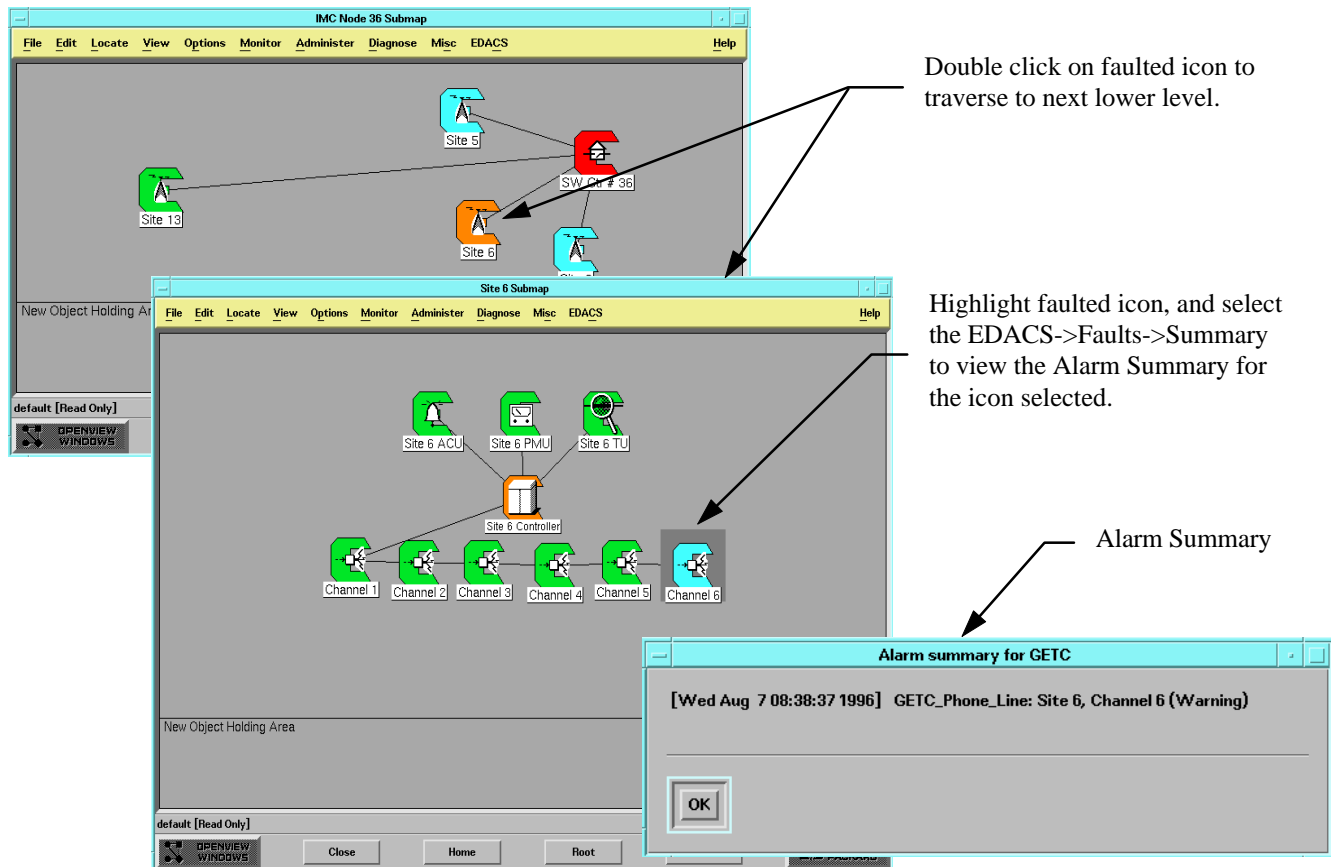
Figure 10 - Using Hierarchical Maps to Identify Fault Events

device polling will be displayed. The display is in a short report (list) format, with each entry in the report listing the time stamp, alarm description, and severity level of the event.

5. If an object in the map has an operational status color other than normal or unknown, it is likely that events have been generated from that object. To access event information for these objects, select the object in the map and then access the menu item **Monitor -> Events**. This will bring up the All Events Browser filtering out all events except those for the selected object.

   NOTE: If the All Events Browser window appears empty, it may be due to the incorrect filter settings or previous deletion of events related to the object. To set the filter, open the **View -> Set Filters** and set the desired filters. To access previously deleted events for the node, use the menu item **File -> Load Event Log -> Filtered**.
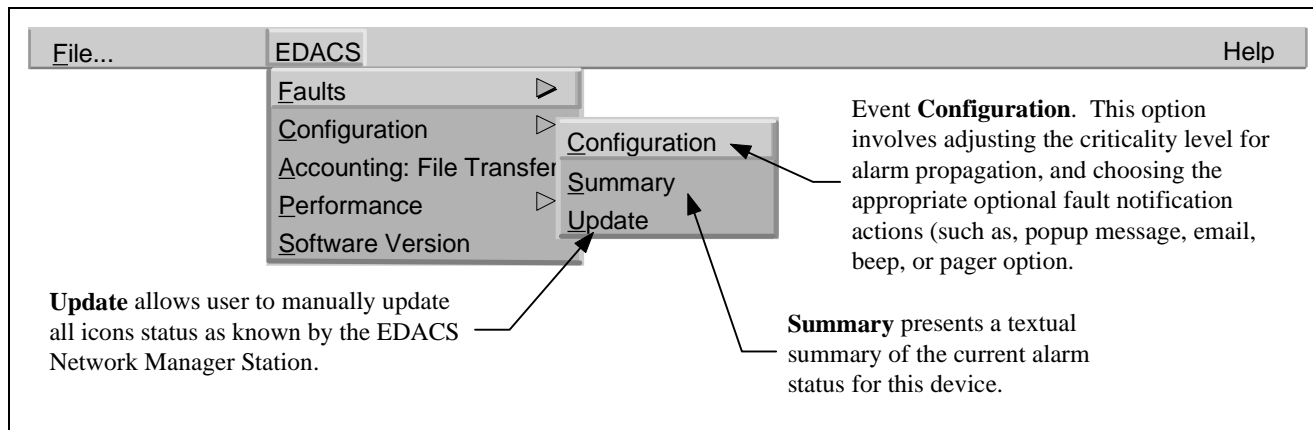
Figure 11 - EDACS Fault Menu

8.3.2 Using The OpenView Event Browser

The Event Browser allows the user to perform the following activity:

- Browse incoming events and events contained in the events log.

- Filter displayed events based on severity, time, source, message and or event type.

- Get event help.

By using the Event Browser you can gain insight into the source and types of events, and isolate and correct problems that have generated events. If you have a read-only Event Notification Interface and delete any events, the deleted events will reappear next time the Interface is started, since deleted events are not saved from a read-only Interface.

Each category in the Event Category has its own Event Browser window. The Event Browser window contains a scrolled list of events belonging to the associated category. Events are displayed in different fonts, based on their severity These fonts can be modified, but by default critical and major severity events are displayed in bold font. The Event Browser window also contains status on the number of events in the window, their severity, and any filtering information.

The Event Browser window lists all undeleted events for the indicated category. The events are in chronological order with the most recent event at the bottom of the list.

For each event, the list shows the following.

- Severity   The severity of the event.

- Date/Time   The day of the week, date and time when the event occurred.

- Source   An identifier (such as a node name) for the network object where the event originated.

- Message   A brief description of the event.

8.3.2.1 Notification of New Events

To know when events have been received, examine the event notification indicator lights in the Event Categories window. The indicator lights will change to corresponding color of the most severe alarm logged.

To see new events as they arrive (real time), open up the EDACS or All Events Browser. Place the scroll bar at the bottom of the browser list; as new events arrive, they are appended to the end of the list.

A listing of EDACS events may be found in LBI-39215. According to the established naming convention, each event name is prefaced with letters that generally represent the reporting EDACS device. See Table 2 for the Letter associations.

8.3.2.2 Selecting Events Within a List

To perform an operation on specific events, select events by clicking the mouse button when the pointer is on top of them. When an event is selected, the text appears in reverse video.

- To select one event, use the mouse select button (usually left button) to click on the event line. This action deselects all other events.

- To select multiple events that are not next to each other in the list, press [CTRL] and hold it down, and then use the mouse select button to select the events you want. This action enables you to select additional events without deselecting the others.

- To select a contiguous range of events, press the mouse select button while dragging the pointer across desired events. This action deselects all events outside the range.

Table 2 - Event Naming Convention Prefix

Letter Designations	EDACS Device
PI	Jessica PBX Interface
BC	BCU/CAL
SM	System Manager
IM	CEC/IMC Manager for NT
CI	CEC/IMC/StarGate
SC	Site Controller
GETC	GE Trunking Card
ACU	Alarm and Control Unit
PMU	Power Monitor Unit
TU	Test Unit

- To toggle a range of events, press [CTRL] and the mouse select button while dragging the pointer across events you want toggled. This action does not affect events outside the range.
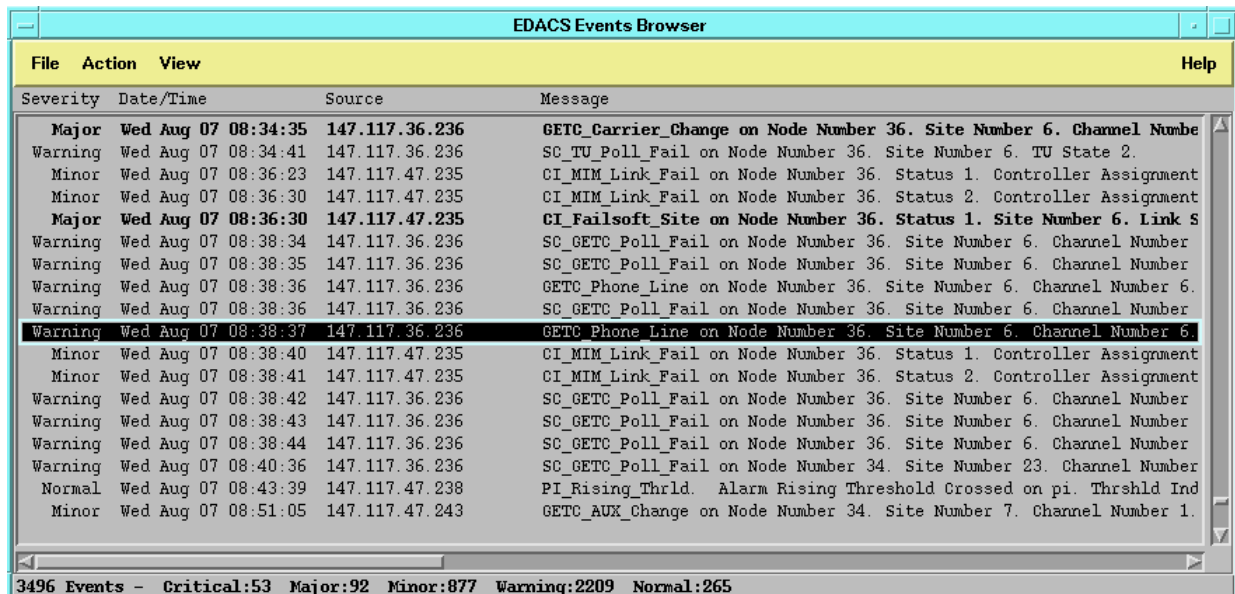
Figure 12 - EDACS Event Browser Example

8.3.2.3 Deleting Events

Events continue to appear in an Event Browser list until you delete them or the maximum number of events for the browser has been reached. The primary reason to delete events is so you can determine when new events occur. If you do not delete events, the buttons in the Event Category window will continue to show status color, and you will not know when newer events of the same or lower severity level occur. If you want to keep the event, but not delete it, you can assign it to a new category or new severity level. In this way you can "acknowledge" the receipt of the event, but keep the event around to look at later. If you have installed the Network Node Manager product, you can create a new category using the event configurator. Call this new category "Acknowledged Events", and assign acknowledged events to that category.

Once deleted, the same events does not re-appear. Though an event will appear in an event category list and the "All Events" category list, you need only delete the event from one list.

8.3.2.4 Filtering Events

Within any Event Browser window, you can filter based on one or more criteria. These criteria are severity, source, and/or event. You use filtering to reduce the number of events displayed. The status of the filtering is shown at the bottom of the Event Browser window, showing how many events are in the category, as well has how many of each severity are displayed. If filtering is on, the status will change to indicate that a subset of the events in the category is displayed. You can then perform operations based on the filtered events, the selected events, or all the events in the category.

As an example, to see all the Critical events:

1. Select the "All Events" category.

2. From the "All Events Browser" pick **View -> Set Filters...**, then chose Critical severity.

You now see all the critical events. After resolving all these events, you will want to delete them.

3. If you select **Action ->Delete -> Filtered Events**, the event category indicator light will change from red to the next most severe color.

8.3.2.5 Locating Source of Event

To locate the source of a specific event perform the following:

1. Select the event and then choose **Action->Highlight Source on Map**.

    This will bring up a submap containing the source of the event. The label for the source object will be highlighted.

2. Select the source object and use the menu items in the OVW map menu bar to obtain more information or to fix the problem that has caused the event.

8.3.2.6 Obtaining Detailed Event Information

Use the following procedure to obtain additional detailed information regarding the cause of the alarm and possible corrective action:

1. Highlight the event, and select the **View->Event Description** from the Event Browser menu bar.
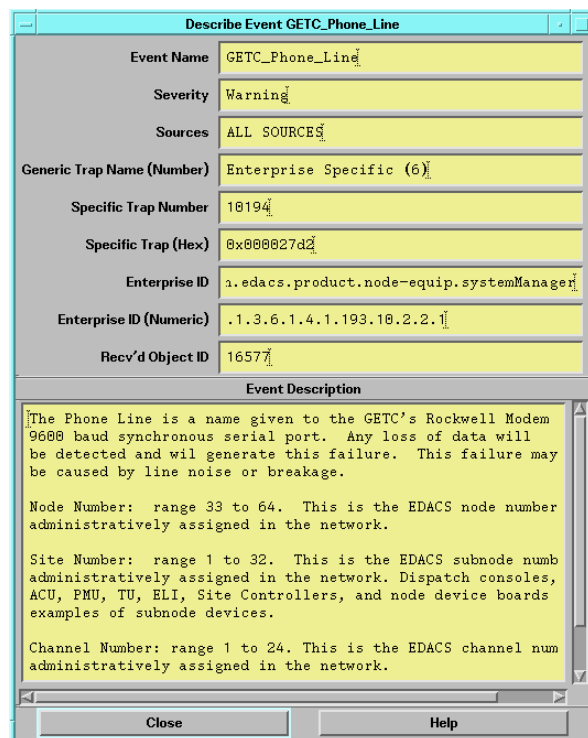
Figure 13 - Event Description

The Network Manager will display the Event Description window providing the technical details associated with the event and possible corrective action.

2. If the event is associated with a site, the user may optionally consult the System Manager Alarm Control Display (screen 40) using the Telnet features described later in this manual.

9. CONFIGURING EDACS DEVICES

The Network Manager provides a single point of control and can configure devices by either bringing up clients running on the Network Manager or by logging into devices with the native access mode. The PI, BCU/CAL, and EDG are accessed in the native access mode. These devices do not have local editors. The Accounting: File Transfer (ftp) menu item may be used to move configuration files to the Network Manager for editing and then transferred back to the device.

The EDACS Configuration Menu presents configuration functions associated with the EDACS device represented by the icon. The following submenus are accessible from the Configuration menu.

- **Configure**:   Brings up the local client Graphical User Interface to configure the device.

- **Connect**:   Connects to the EDACS device (i.e., via Telnet) to use the device's native configuration utilities.

- **Reboot**:   Automatically reboots the EDACS device.

- **Restart**:   Restarts traffic after a shutdown.

- **Shutdown**:   Shuts down traffic without losing connectivity.
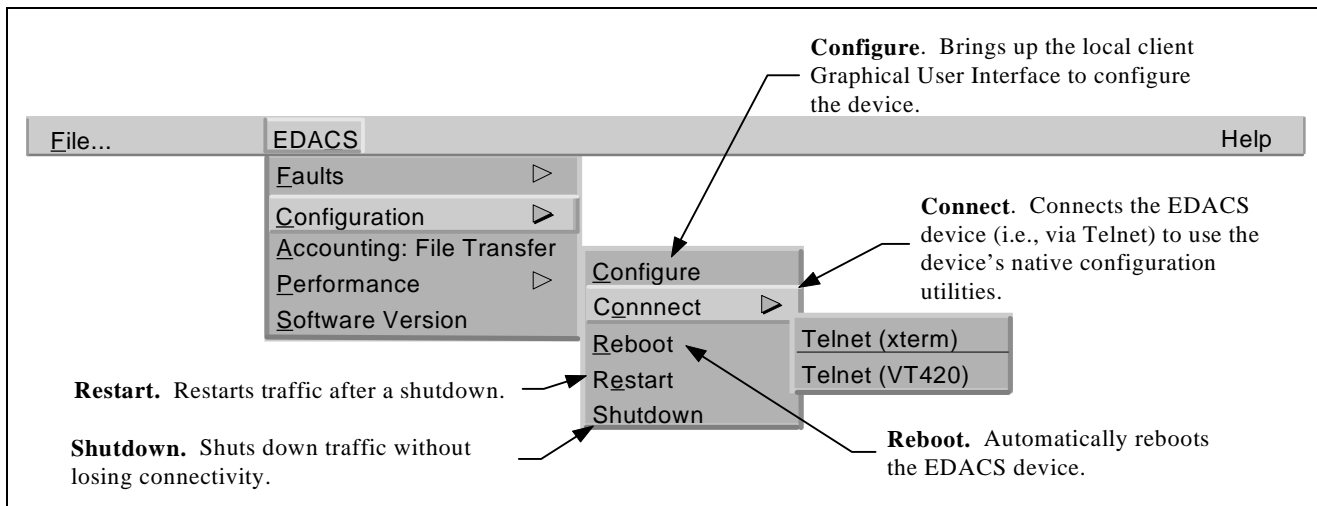
Figure 15 - EDACS Configuration Menu

9.1 INTEGRATED CEC/IMC MANAGER

The CEC/IMC Manager client is invoked using the **EDACS->Configuration->Configure** menu item with the IMC Manager icon selected. The CEC/IMC Manager for Windows NT employs the client-server paradigm. The server, which interfaces to the CEC/IMC, runs on the Windows NT platform while the client may run on either the Windows NT platform or the EDACS Network Manager UNIX platform. The CEC/IMC Manager HP-UX client has the ability to dynamically change between the Motif and Windows environment appearance. The CEC/IMC Manager communicates from its Graphical User Interface (GUI), or client, to its underlying engine via Open Systems Foundation (OSF) compliant Remote Procedure Calls (RPCs). This strategy implies that if the Ethernet link between the IMC Manager and the EDACS Network Manager goes down (which should be highly unlikely), then the EDACS Network Manager interface for the IMC will only be able to report that the link is down.
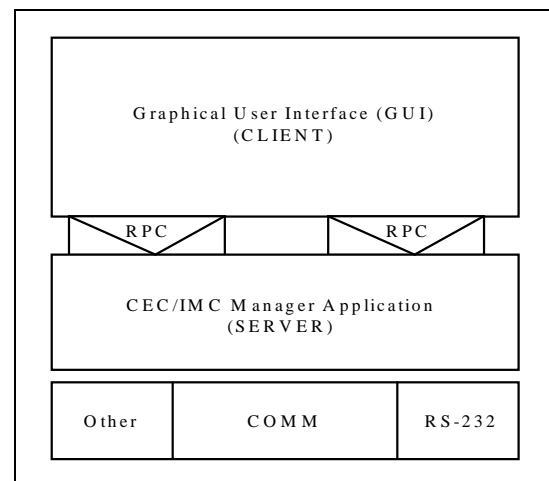
Figure 14 - CEC/IMC Client-Server Paradigm

9.1.1 Starting The CEC/IMC Session

From the Network Manager, invoke the CEC/IMC Manager client using the following procedure:

1. On the Switch Center submap, highlight the IMC Manager icon.

2. From the Main Menu bar, select the **EDACS->Configuration->Configure** menu item. The Network Manager will display the CEC/IMC Manager HP-UX Client dialoag box indicating that the CEC/IMC Client is initializing. NOTE: The CEC/IMC Manager program must be running for this process to succeed. (Refer to LBI-39224, EDACS CECX/IMC Manager, Version 5.0 for Windows NT if required.)

3. From the CEC/IMCManager HP-UX Client dialog box, click on **OK**. This brings up the the CEC/IMC Manager main menu (Figure 16).

    The bottom status bar displays several messages that are helpful or important to the CEC/IMC Manager user. "For Help, press F1" or the current menu choice and the current time are displayed at each end of the status bar. System status—"No System Errors" or "System Errors"—and Link status—"Mom Link is Up" or "Mom Link is Down"— provide the user with important information concerning system operation.
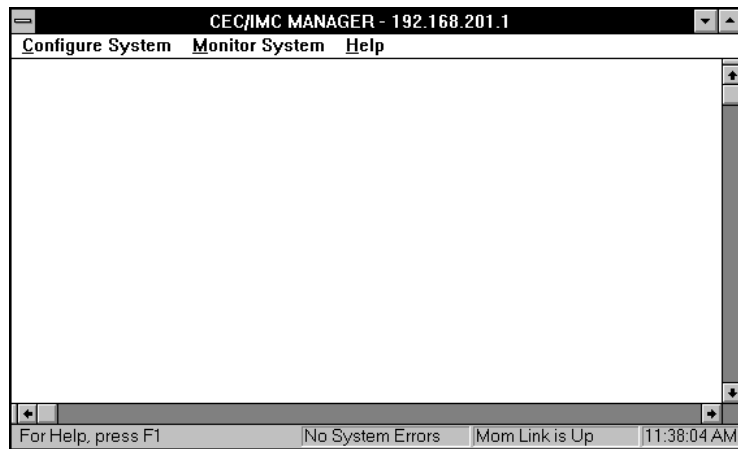
Figure 16 - CEC/IMC Manager Main Window and Menu Bar

4. Select one of the CEC/IMC functions from the Menu Bar.

    Selecting any of the choices from the CEC/IMC Manager menu bar (Configure System, Monitor System, Help) will display the Login dialog box. You will be prompted to enter a user name and password before execution of the program will continue. The default user name is "NMUSER" and the default password is "GUEST." These log-in defaults are provided in the PASSWORD.DAT file that is part of the CEC/IMC Manager installation.
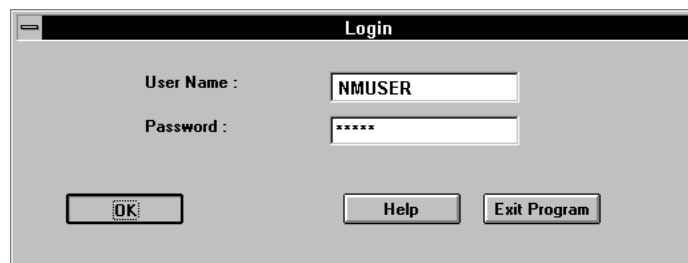
Figure 17 - CEC/IMC Manager Login

Before proceeding, it is recommended that the user be completely familiar with using the CEC/IMC Manager for Windows NT. Complete instructions may be found in LBI-39224.

9.1.2 Sample CEC/IMC Manager Screens

Some sample CEC/IMC Manager screens for configuration follow.
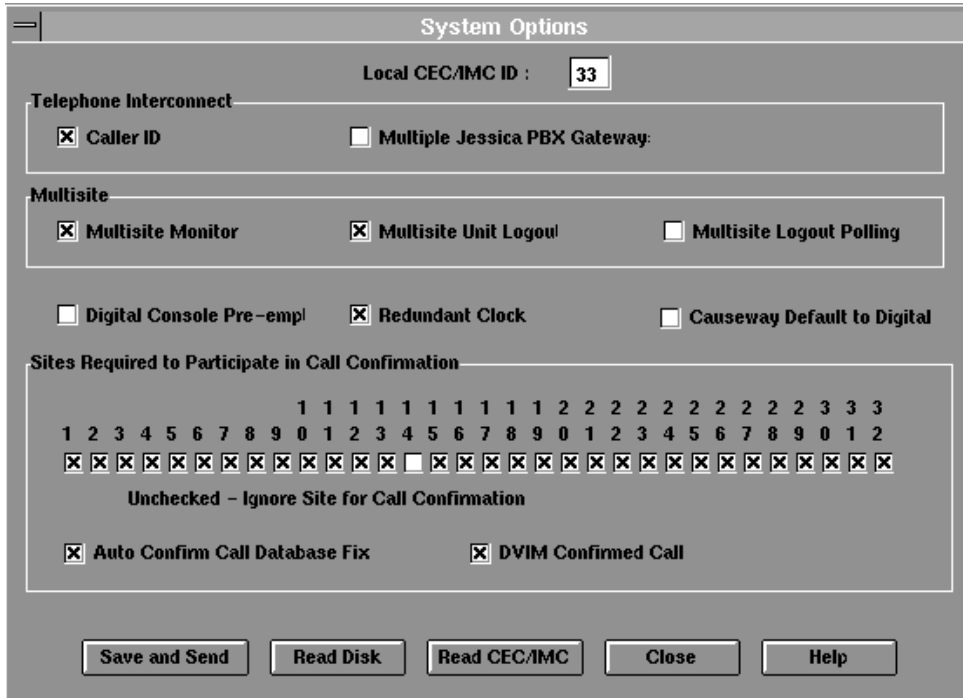
Figure 18 - System Options for Digital Console Pre-empt Example Screen
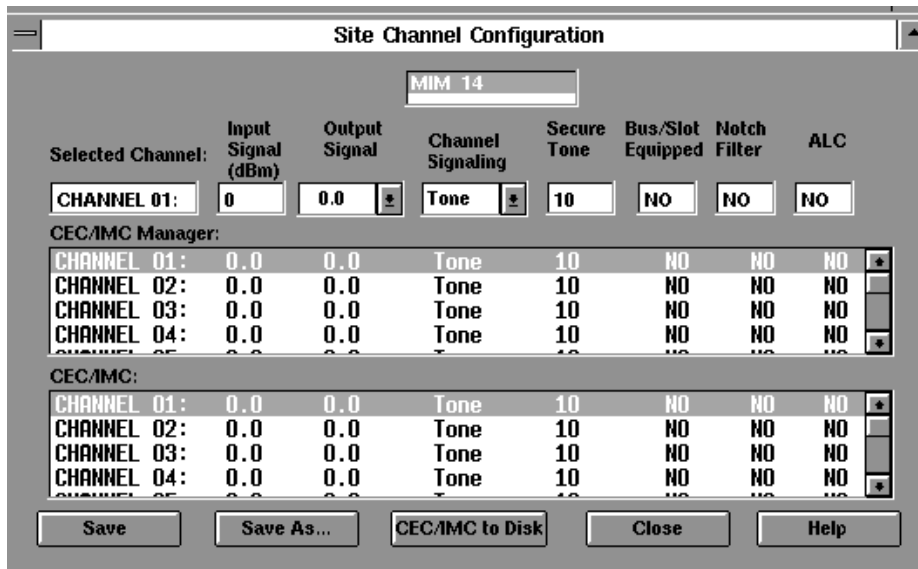
Figure 19 - Site Channel Configuration Example Screen

Figure 20 - Console User Profile Configuration Example Screen

9.2 TELNET SESSIONS TO THE PI, BCU, CAL, AND EDG

Telnet access into each device is password-protected. Therefore, the user requesting access must have login privileges for the remote device. The normal Telnet capability of the HP workstation provides VT100 emulation, which is the normal, generic emulation for simple applications. Generic VT100 emulation is used for the PI, BCU, CAL, and EDG for Telnet connections. This level of terminal emulation is bundled with HP-UX.

1. On the Switch Center submap, highlight the device's icon.

2. From the Main Menu bar, select the **EDACS -> Configuration -> Connect -> Telnet(xterm)** menu item.

3. Enter the your username and password to gain access to the device. Refer to the device's User manual for additional information.

9.3 TELNETING TO THE SYSTEM MANAGER

Telneting to the System Manager uses VT220 emulation because it is a VAX/VMS system running a screen-oriented application. From the Network Manager, invoke the System Manager program using the following procedure:

1. On the Switch Center submap, highlight the System Manager icon.

2. From the Main Menu bar, select the **EDACS -> Configuration -> Connect -> Telnet (VT420)** menu item.

   The Network Manager will display the System Manager log on screen as shown in Figure 21.

3. Enter the Username (default Username is "EGESYSMGR") and press the **<Enter>** key.

4. Enter the Password (default Password is "EGESYSMGR") and press the **<Enter>** key.

This brings up the the System Manager User Menu screen (Figure 22). From this point on all System Manager operations are as described in LBI-38984.

NOTE

When telneting into the System Manager, the keyboard is remapped for use with the VAX/VMS operating system. A keyboard template (AE/LZT 123 1908/1) is available and may be ordered through our publications department.
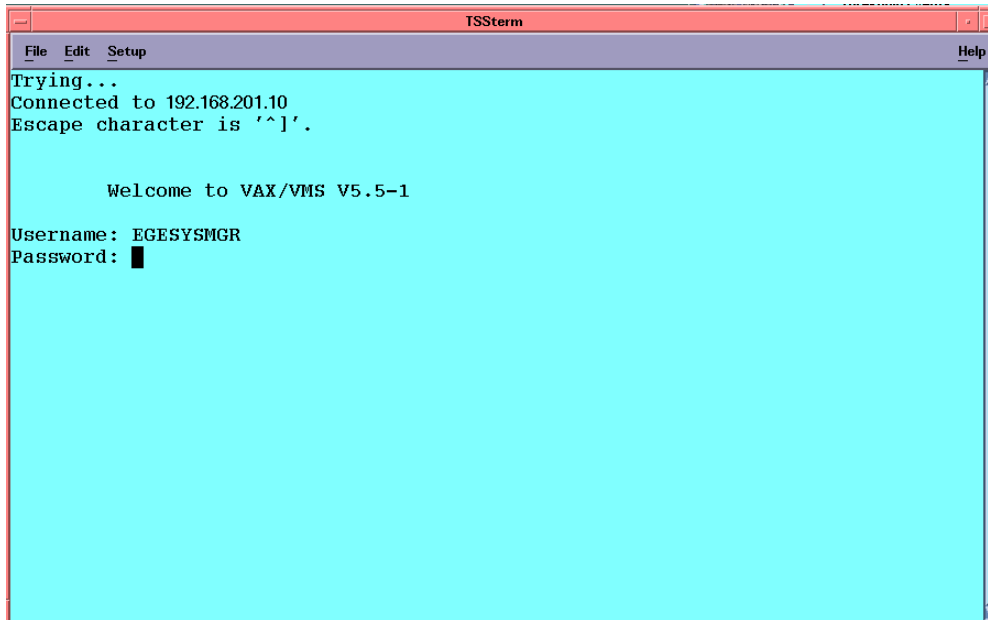
Figure 21 - System Manager Login Screen
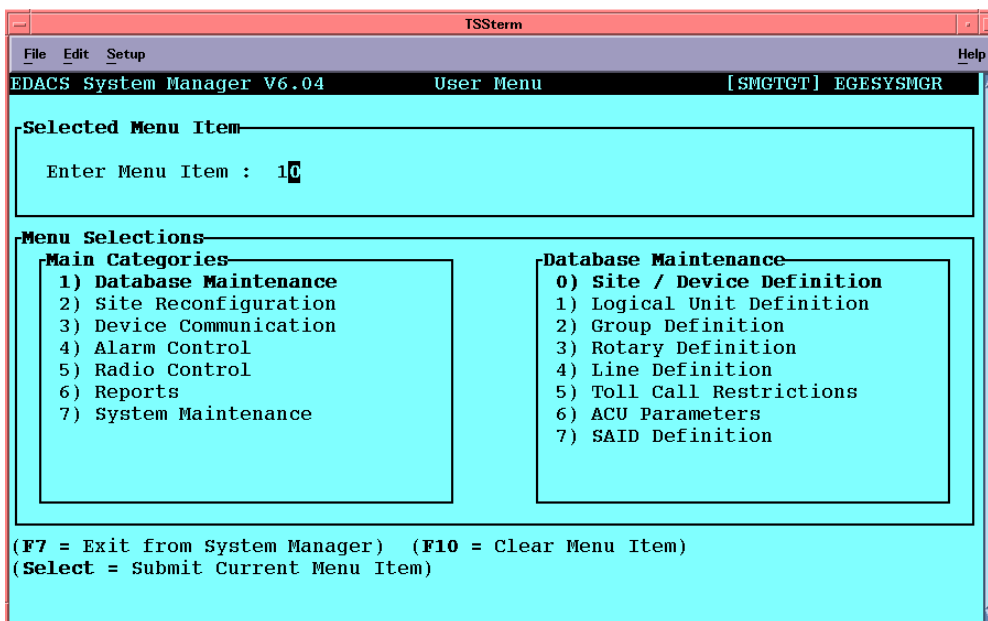
Figure 22 - System Manager User Menu

9.4 USER ACTION LOGGING

The EDACS Network Manager logs the EDACS Configuration functions reboot, restart, and shutdown. Each logged action includes the host name, user name, time, date, description of action, and targeted EDACS IP Address. User action log information is written to the same file displayed by the Event Browser.

10. TRANSFERRING DEVICE FILES

Occassionally, it may be necessaary to transfer device files; such as configuration files for editing, activity data for billing, etc. Device files may be transfered from the device's storage location to a more easily accessible location by using the Accounting: File Transfer function. This process allows the Network Manager to connect to the EDACS device and initiate a file transfer using File Transfer Protocol (ftp), thus allowing device-specific accounting records or files to be transferred to another location (such as the user's home directory) for use by the EDACS Network Manager or a third party billing package.

The following figures provide examples of FTP sessions on the PI, BCU and System Manager. In these examples, the activity data is transfered via FTP, using a GET command, for use with another program. A listing of FTP commands is available in LBI-38987 and LBI-38963.

1. Highlight the device's icon on the Network Manager's submap.

2. From the Main Menu bar, select the **EDACS -> Accounting: File Transfer** menu item.

    The Network Manager will display the devices login prompt. In all cases, it will be necessary to enter your User name and Password before proceeding with the transfer.

NOTE

Files are transferred to the directory OpenView is invoked from. This is usually the user's home directory. If, however, OpenView is invoked from the command line in a write protected directory, then the file transfer will fail.

PI Activity Data Transfer Example

This is an example of transferring the PI activity record *sep01.log* to the users HOME directory.

```
Connected to 192.168.201.30.
220 192.168.201.30 pSOSystem FTP server (NTL68K/1.0.4) ready.
Name (192.168.201.30:lab): user
331 Password required for user.
Password:
230 User user logged in.
Remote system type is pSOSytem.
ftp> cd activity
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for ..
-rwxrwxrwx   1 root     194684 Sep 01 1996 23:44 sep01.log
-rwxrwxrwx   1 root     207286 Sep 02 1996 23:47 sep02.log
-rwxrwxrwx   1 root     619989 Sep 03 1996 23:09 sep03.log
-rwxrwxrwx   1 root      12241 Jan 30 1996 16:07 fatal.log
-rwxrwxrwx   1 root     737526 Sep 04 1996 23:16 sep04.log
-rwxrwxrwx   1 root     324909 Sep 05 1996 13:35 sep05.log
-rwxrwxrwx   1 root     286160 Feb 08 1996 14:00 summary.log
-rwxrwxrwx   1 root       5318 Jun 06 1996 14:05 error.log
-rwxrwxrwx   1 root    2621385 Jan 17 1996 17:25 isdx.log
-rwxrwxrwx   1 root       9180 Aug 30 1996 16:34 isdn.log
WARNING! 10 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
ftp> get sep01.log
200 PORT command successful.
150 Opening ASCII mode data connection for sep01.log (194684
bytes).
226 Transfer complete.
197586 bytes received in 9.18 seconds (21.03 Kbytes/s)
ftp> bye
```

Figure 23 - Transferring PI Activity Data Using FTP

BCU CDR Data Transfer Example

This is an example of transferring a CDR record, *t2250609.CDR,* from the BCU to the user's home directory. The user may then use a third party application that reads CDR records.

```
Connected to 192.168.201.20.
220 192.168.201.20 pSOSystem FTP server (NTL68K/1.0.4) ready.
Name (192.168.201.20:lab): user
331 Password required for user.
Password:
230 User user logged in.
Remote system type is pSOSytem.
ftp> cd cdr
ftp>ls
200 PORT command successful.
150 Opening ASCII mode data connection for ..
-rwxrwxrwx   1 root    176803 Aug 12 1996 23:59 t2250609.CDR
-rwxrwxrwx   1 root     34001 Aug 10 1996 23:59 t2230051.CDR
-rwxrwxrwx   1 root   2574762 Aug 15 1996 23:59 t2272359.CDR
-rwxrwxrwx   1 root   1625170 Aug 17 1996 23:59 t2292359.CDR
-rwxrwxrwx   1 root   2944632 Aug 14 1996 23:59 t2262359.CDR
-rwxrwxrwx   1 root     22736 Aug 18 1996 23:59 t2310018.CDR
-rwxrwxrwx   1 root    906761 Aug 16 1996 23:59 t2290647.CDR
-rwxrwxrwx   1 root    411755 Aug 19 1996 23:59 t2320008.CDR
-rwxrwxrwx   1 root    208131 Aug 20 1996 23:59 t2322359.CDR
-rwxrwxrwx   1 root    214850 Aug 21 1996 23:59 t2340002.CDR
-rwxrwxrwx   1 root    182558 Aug 22 1996 23:59 t2350122.CDR
-rwxrwxrwx   1 root    206159 Aug 23 1996 23:59 t2360025.CDR
-rwxrwxrwx   1 root     31337 Aug 24 1996 23:59 t2370001.CDR
-rwxrwxrwx   1 root     61214 Aug 25 1996 23:59 t2380025.CDR
-rwxrwxrwx   1 root    145377 Aug 26 1996 23:59 t2390704.CDR
-rwxrwxrwx   1 root    211990 Aug 27 1996 23:59 t2392359.CDR
-rwxrwxrwx   1 root    116084 Aug 29 1996 23:59 t2421216.CDR
-rwxrwxrwx   1 root      1295 Aug 28 1996 14:10 t3401651.CDR
-rwxrwxrwx   1 root       174 Aug 29 1996 12:16 t3411457.CDR
-rwxrwxrwx   1 root    105984 Sep 05 1996 13:46 t2490040.CTM
-rwxrwxrwx   1 root    241220 Aug 06 1996 23:59 t2190020.CDR
-rwxrwxrwx   1 root    175904 Aug 07 1996 23:59 t2200014.CDR
-rwxrwxrwx   1 root    202655 Aug 08 1996 23:59 t2210026.CDR
-rwxrwxrwx   1 root    157541 Aug 09 1996 23:59 t2220015.CDR
-rwxrwxrwx   1 root     21800 Aug 11 1996 23:59 t2232359.CDR
-rwxrwxrwx   1 root    878304 Aug 13 1996 23:59 t2252359.CDR
-rwxrwxrwx   1 root    145408 Aug 28 1996 14:03 t2410004.CDR
-rwxrwxrwx   1 root    162410 Aug 28 1996 23:59 t2411410.CDR
-rwxrwxrwx   1 root    198611 Sep 03 1996 23:59 t2470205.CDR
WARNING! 35 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
ftp>  get t2250609.CDR
200 PORT command successful.
150 Opening ASCII mode data connection for t2250609.CDP (176803 bytes).
226 Transfer complete.
178936 bytes received in 8.04 seconds (21.73 Kbytes/s)
ftp> bye
```

Figure 24 - Transferring a BCU Billing Record Using FTP

System Manager Activity Data Transfer Example

   This is an example of transferring an Activity data file, *ACT_01-SEP-1996.03;1,* from the System Manger to the user's home directory. The user may then use a third party application that reads CDR records.

```
Connected to 192.168.201.10.
220 smgtgt MultiNet FTP Server Process V3.5(15) at Thu 5-Sep-96 2:09PM-EDT
Name (192.168.201.10:lab): egesysmgr
331 User name (egesysmgr) ok. Password, please.
Password:
230 User EGESYSMGR logged into DKA300:[EGESYSMGR] at Thu 5-Sep-96 2:09PM-EDT, job
23c
Remote system type is VMS.
ftp> dir
200 Port 10.30 at Host 147.117.47.240 accepted.
150 List started.


DKA300:[EGESYSMGR]

ERRLOG.DAT;3       1429  14-MAY-1996 09:41 [1,1] (RWED,RWED,RWED,)
ERRLOG_SUPPORT_OFF.COM;5   1  16-AUG-1994 21:32 [1,1] (RWED,RWED,RWED,)
ERRLOG_SUPPORT_ON.COM;15   1  16-AUG-1994 21:31 [1,1] (RWED,RWED,RWED,)
FTP_SERVER.LOG;1     0   5-SEP-1996 14:09 [1,1] (RWED,RWED,RE,)
LOGIN.COM;32  2   7-AUG-1996 09:38 [1,1] (RWED,RWED,RE,)
NETSERVER.LOG;2      5   1-MAR-1994 18:40 [1,1] (RWED,RWED,RE,)
UNTDIS_DEBUG.TXT;3   1  23-APR-1993 09:29 [1,1] (RWED,RWED,RWED,)

Total of 1439 blocks in 7 files.
226 Transfer completed.
ftp> cd smact:
250 Connected to EGE_SMACTROOT:[SMACT].
ftp>  dir *sep*
200 Port 10.59 at Host 192.168.201.2 accepted.
150 List started.


EGE_SMACTROOT:[SMACT]

ACT_01-SEP-1996.03;1   102   1-SEP-1996 12:26 [1,1] (RWED,RWED,RE,)
ACT_01-SEP-1996.04;1   612   1-SEP-1996 00:18 [1,1] (RWED,RWED,RE,)
ACT_01-SEP-1996.05;1   102   2-SEP-1996 16:41 [1,1] (RWED,RWED,RE,)
ACT_01-SEP-1996.06;1   408   1-SEP-1996 00:11 [1,1] (RWED,RWED,RE,)
ACT_02-SEP-1996.04;1   612   2-SEP-1996 01:50 [1,1] (RWED,RWED,RE,)
ACT_02-SEP-1996.05;1   102   2-SEP-1996 16:41 [1,1] (RWED,RWED,RE,)
ACT_02-SEP-1996.06;1   408   2-SEP-1996 01:09 [1,1] (RWED,RWED,RE,)
ACT_05-SEP-1996.06;1   204   5-SEP-1996 00:57 [1,1] (RWED,RWED,RE,)

Total of 3774 blocks in 14 files.
226 Transfer completed.
ftp>  get ACT_01-SEP-1996.03;1
200 Port 10.60 at Host 192.168.201.2 accepted.
150 ASCII retrieve of EGE_SMACTROOT:[SMACT]ACT_01-SEP-1996.03;1 started.
226 Transfer completed.  7038 (8) bytes transferred.
7038 bytes received in 0.59 seconds (11.73 Kbytes/s)
ftp> bye
```

Figure 25 - Transferring System Manager Activity Data Using FTP

11. MONITORING PERFORMANCE TRENDS

Performance trends can be used to determine utilization and accessibility or to tune system performance. Trends can be viewed on a per site or Radio Switch basis. The results of these trends are presented on the 2-D line graphs.

This data collection feature allows individual data trend items to be monitored for exceeding a user defined threshold. The data points used in the trend may be saved or discarded. Popup messages or automatic actions can occur, such as email message, when a threshold is exceeded. NOTE: If data points are saved then disk space must be monitored.

The EDACS Network Manager Performance menu provides 2-D line graphs that measure the overall node and site level performance via various predefined groupings of performance parameters.

- **Utilization**:   Provides totals for call types pertaining to this EDACS device.

- **Accessibility**:   Displays queued, busy, and denied call information for this EDACS device.

- **Compare**:   Displays a single MIB value for multiple nodes or sites.

The EDACS Performance Menu presents performance information about the EDACS device represented by the icon. **NOTE:** In the Performance menu items shown below the choices for node and site are the same; therefore, only the node path is shown.

NOTE

All performance parameters are from the perspective of the CEC/IMC.

The performance graphs and call activity initiated from the Main Menu bar may get performance data from several sources. The following hierarchy will be used to determine the source of the data:

- BCU/CAL platform

- Jessica PI platform

NOTE

Real-time system monitoring requires a PI or a BCU/CAL on the node being monitored.

11.1 USING TWO-DIMENSIONAL LINE GRAPHS

Most of the functions presented in the menu require the user to select one or more icons from one or more of the OpenView maps.   In order to select a single icon, the user simply clicks the left mouse button. To select multiple items, the user clicks the left mouse button and "drags" a rectangular area in which all items within the rectangle will be selected. Once items have been selected, then the user may add specific icons to the selection by holding down the CTRL key while clicking the left-most mouse. Node level 2-D line graphs (summarizes traffic at a node) and site level 2-D line graphs (summarizes traffic at a site) may be produced for Utilization, Accessibility, and Compare Performance menu items.

Node Performance line graphs may be invoked from the following icons: IMC Node, CEC Node, IMC, and CEC. Site Performance line graphs and call activity may be invoked from the following icons: IMC Node, CEC Node, IMC, CEC, Site, and PI.

The user may select a set of one or more icons and invoke the desired performance graph. For instance, if the user selects several nodes, then a graph for each of the different nodes will be produced. One graph per valid icon selected will be initiated.

11.1.1 Line Graph Example

The example of a line graph, shown in Figure 26, illustrates the ease and clarity with which the EDACS Network Manager platform presents data. The performance groupings display logically similar performance items on one graph, depicting each variable in a different color.
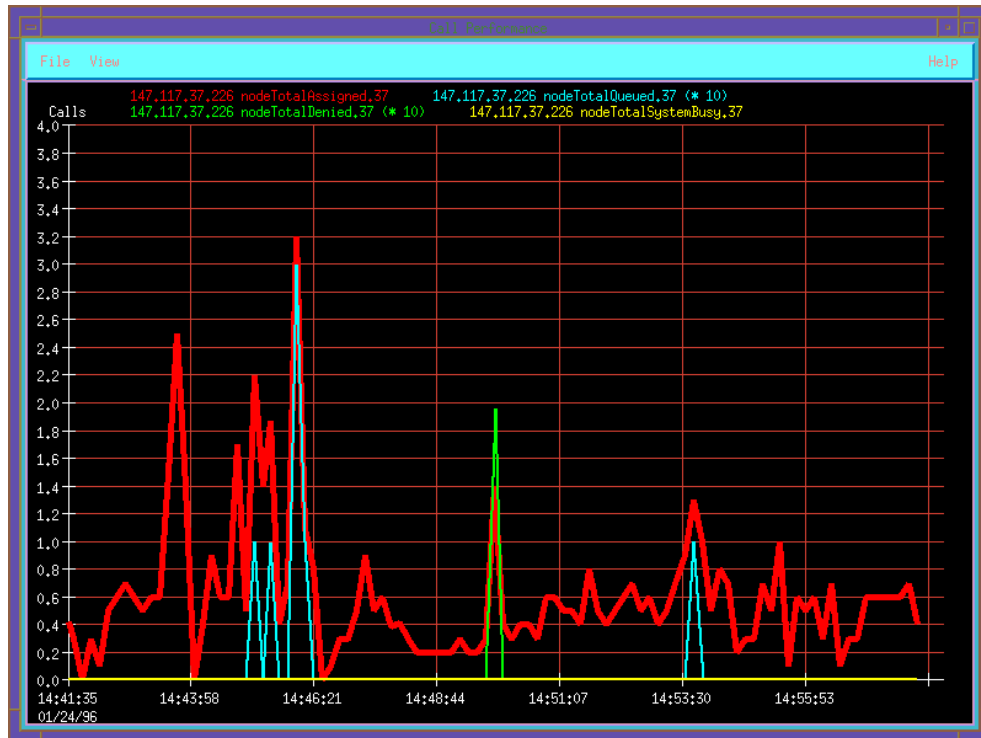
Figure 26 - Example of a Two-Dimensional Line Graph

11.1.2 Customizing Line Graphs

When a performance item is selected from the Main Menu, a default 2-D line graph appears. Pull-down menu items are available for the following selections:

1. Statistics (activate a statistics window with raw statistics information).

2. Sampling interval (range is 1 sec to months).

3. Sampling items (line graph items may be individually turned on/off).

4. Data capture option (i.e., store graph data in database).

5. Print option.

6. Line width.

7. Scaling

The ability to zoom in and out, and scroll back and forth, within the areas of interest in the line graph comes standard with OpenView Network Node Manager. The OpenView Network Node Manager graph display program is called "xnmgraph." Under the file menu is a print command. This causes the entire window to be printed out in "xwd" format, but the window can also be redirected to a file. Many off-the-shelf programs can read and process xwd format files. Among these are

- HP ImageView (part of the Mpower package)

- Xview (public domain software)

Both of these programs will convert the "xwd" format to "TIF" and "GIF" formats which are easily imported into other applications.

11.2 TRACKING EDACS DEVICE UTILIZATION

The **Performance -> Utilization** menu item allows the user to chart the totals for call types pertaining to this EDACS device.

The entries on the Performance sub-bar, see Figure 27, are detailed below. All of the following graphs will be displayed for either nodes or sites.

- Call Performance - Network-wide call performance (totals of all call types) for Channel Assignments, Queues, Denies, and System Busies.

- Channel Assignment - Total Channel Assignments for the following call types: Individual Voice Calls, Group Voice Calls, Individual Data Calls, Group Data Calls, Individual Outbound Interconnect, Individual Inbound Interconnect, Group Inbound Interconnect, and ALL.

- Individual Call - Individual voice call performance totals for Channel Assignments, Queues, Denies, and System Busies.

- Group Voice - Group voice call performance totals for Channel Assignments, Queues, Denies, and System Busies.

- Individual Data - Individual data call performance totals for Channel Assignments, Queues, Denies, and System Busies.

- Group Data - Group data call performance totals for Channel Assignments, Queues, Denies, and System Busies.

- Individual Outbound Telephony - Individual outbound interconnect call performance totals for Channel Assignments, Queues, Denies, and System Busies.

- Individual Inbound Telephony - Individual inbound interconnect call performance totals for Channel Assignments, Queues, Denies, and System Busies.

- Group Inbound Telephony - Group inbound interconnect call performance totals for Channel Assignments, Queues, Denies, and System Busies.
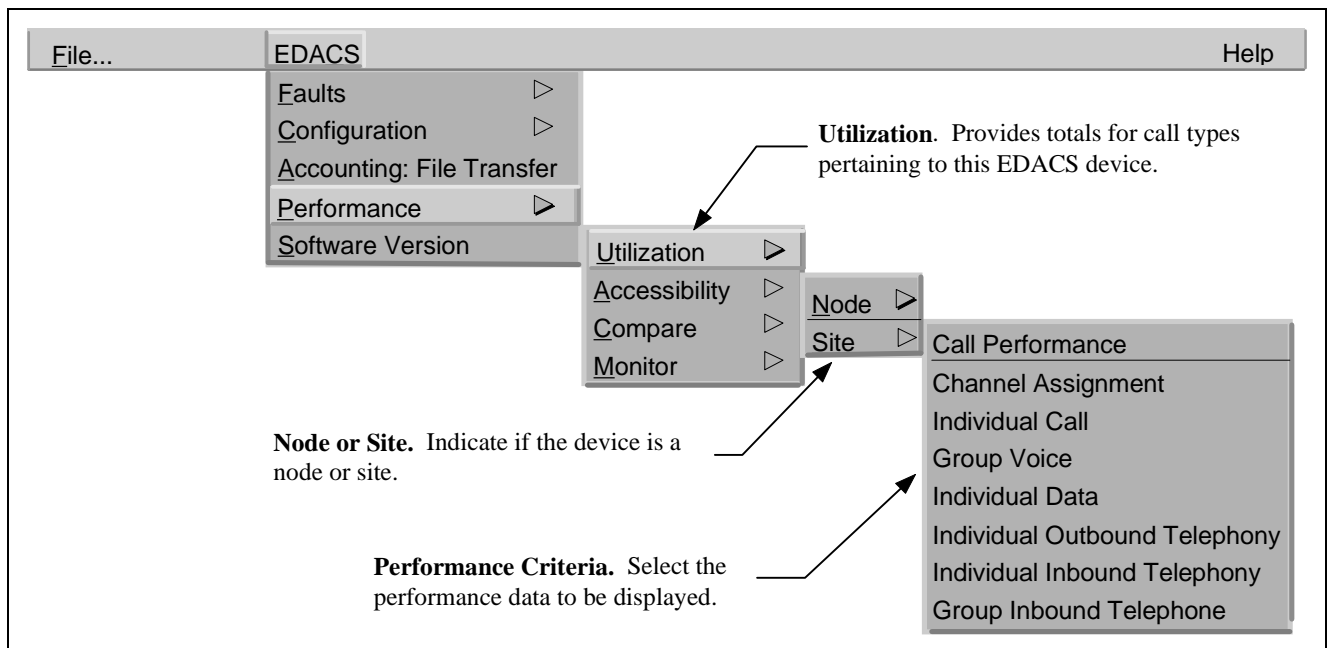
Figure 27 - EDACS Performance -> Utilization Menu

11.3 TRACKING EDACS DEVICE ACCESSIBILITY

The **Performance -> Accessibility** menu item allows the user to chart the queued, busy, and denied call information for this EDACS device.

All of the following graphs will be displayed for either nodes or sites.

- Denies - Total Denies for the following call types: Individual Voice Calls, Group Voice Calls, Individual Data Calls, Group Data Calls, Individual Outbound Interconnect, Individual Inbound Interconnect, Group Inbound Interconnect, and ALL.

- Queues - Total Queues for the following call types: Individual Voice Calls, Group Voice Calls, Individual Data Calls, Group Data Calls, Individual Outbound Interconnect, Individual Inbound Interconnect, Group Inbound Interconnect, and ALL.

- System Busies - Total System Busies for the following call types: Individual Voice Calls, Group Voice Calls, Individual Data Calls, Group Data Calls, Individual Outbound Interconnect, Individual Inbound Interconnect, Group Inbound Interconnect, and ALL.
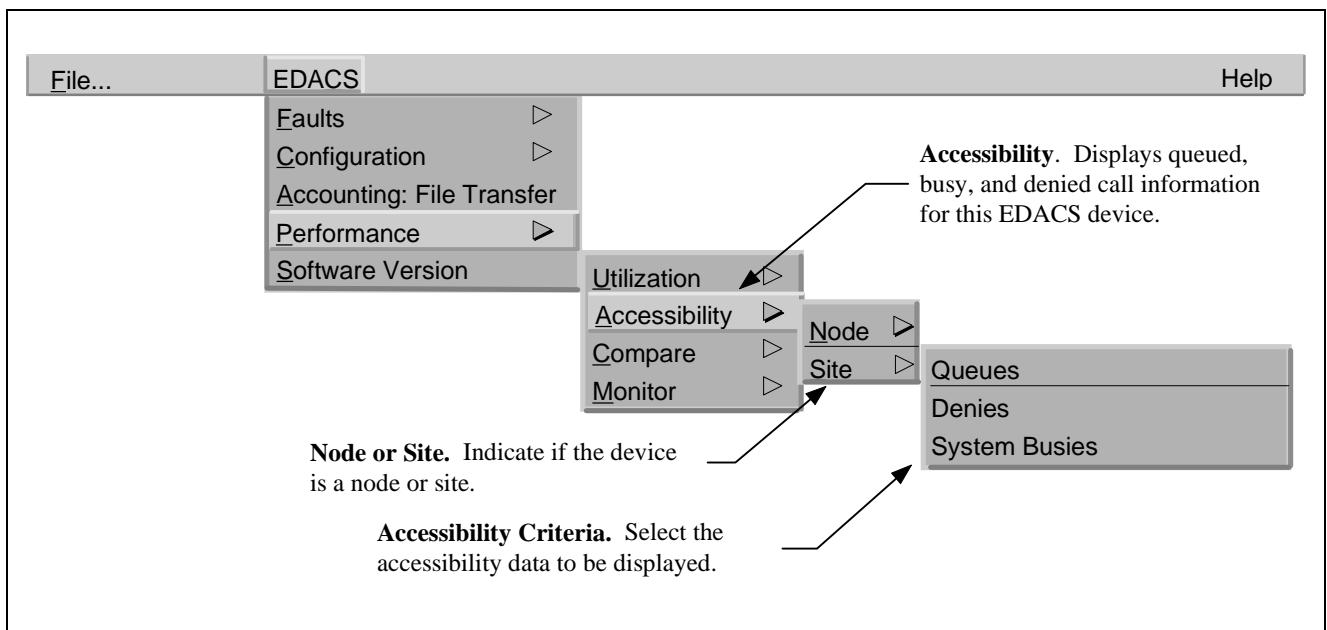
Figure 28 - EDACS Performance / Accessibility Menu

11.4 COMPARING PERFORMANCE FROM MULTIPLE SITES OR NODES

The **Performance -> Compare** menu item allows the user to chart a single MIB value for multiple nodes or sites.

The following graphs will display a single performance parameter for multiple nodes or sites on the same graph. There will be a different line for each of the sites or nodes selected. The sites being displayed can be on different nodes.

- Channel Assignments - Total Channel Assignments for all call types.

- Queues - Total Queues for all call types.

- Denies - Total Denies for all call types.

- Drops - Total Drops for all call types.

- System Busies - Total System Busies for all call types.

- Emergencies - Total Emergencies.

- Secondary Assignments - Total Secondary Assignments for all call types.

- Message Trunks - Total Message Trunk Assignments for all call types.

- Air Time - Total Air Time for all call types.

- Queue Time - Total Queued Time for all call types.

    NOTE: If selecting Airtime with one site selected (minimum number of icons is one for example), then graph Airtime for that site only.
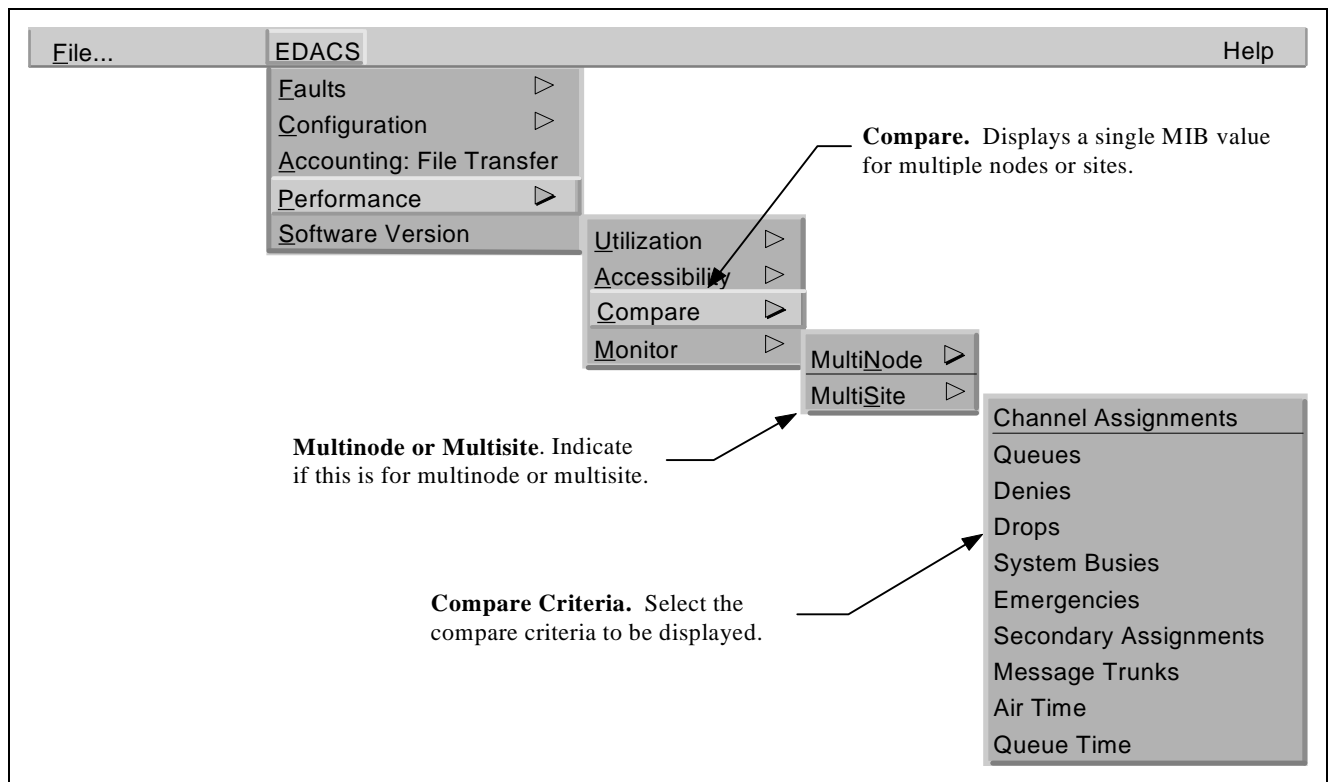
Figure 29 - EDACS Performance -> Compare Menu

12. MONITORING REAL-TIME CALL ACTIVITY

Real-time call activity can be displayed on both node (Multisite Monitor) and site (Site Monitor) levels. In the Multisite Monitor (MSM), active call types are indicated by the application of color to the button representing a particular channel on a particular site. The color is removed when the call has completed. For the Site Monitor (SM), active call types are highlighted, and channel status is indicated in the status column. The originating site may be determined by the color of the button lettering. White button lettering indicates primary "originating" site while gray button lettering indicates secondary sites. NOTE: Forced and Confirmed Calls will show multiple primary sites.

Screen updates are event-driven. An indication that the call has completed at the monitor level does not guarantee that the call has cleared throughout the EDACS infrastructure. Detection of hung channels is not a monitor feature. When the site is in Failsoft, the channel updates on the Multisite Monitor and Site Monitor screens report the last known control channel.

The Multisite Monitor or Site Monitor session is invoked by selecting the desired option from the **Performance -> Monitor** menu item as shown in Figure 30 for monitoring call activity.

- **MultiSite on Node** - Invokes the Multisite Monitor for all applicable sites on each node selected. Operation is valid for the CEC or CEC Node, and IMC or IMC Node (NIM) icon.

- **MultiSite on Sites** - Invokes the Multisite Monitor for all selected sites on the same node as the first node detected. Sites on a different node will be ignored. Operation is valid for the Site icon, PI icon, and CEC or IMC, or CEC Node or IMC Node (NIM) icon.

- **Site** - Invokes the Site Monitor for each site selected. Operation is valid for the Site icon, PI icon, and CEC or IMC, or CEC Node or IMC Node (NIM) icon.

The following sections detail the use and operation of the MultiSite Monitor and the Site Monitor.
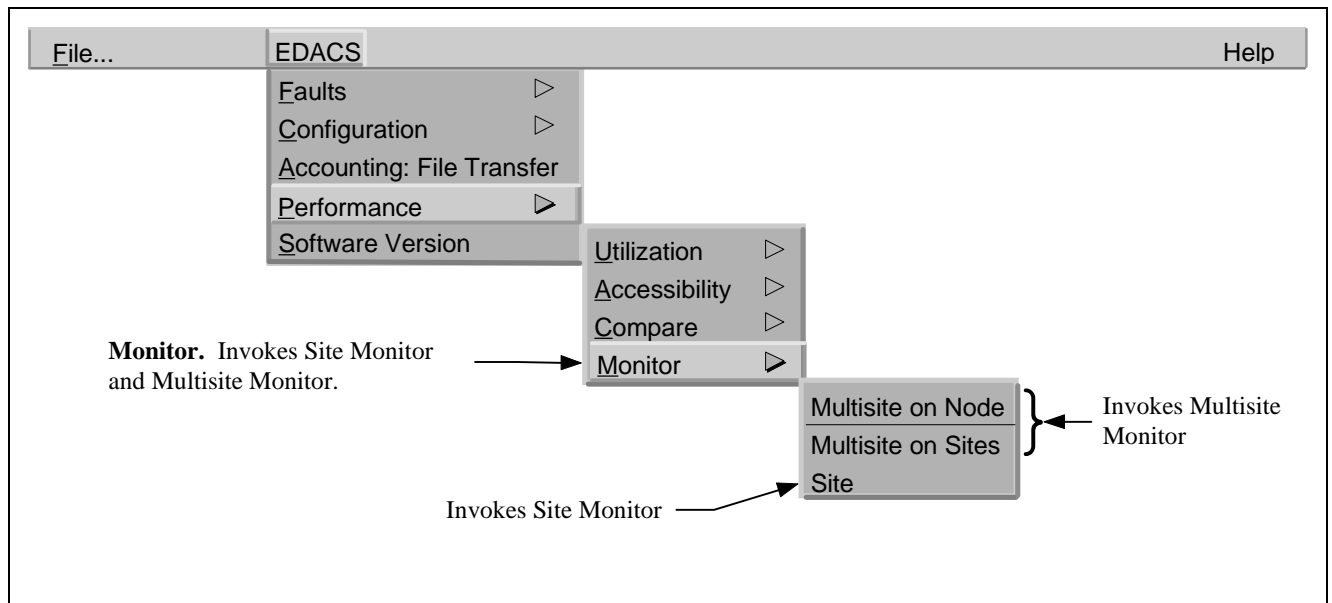
Figure 30 - EDACS Performance -> Monitor Menu

12.1 USING THE MULTISITE MONITOR APPLICATION

The Multisite Monitor application monitors call activity for one user-specified node. All windows can be manipulated (i.e., resized, iconized, closed) via standard window border operations. The Multisite Monitor window contains a main menu bar, work area, and scroll bars (see Figure 31). Vertical and horizontal scroll bars are generated automatically, as needed, for the work area.

The work area portion of the screen is arranged in a row-column matrix with channel numbers along the rightmost and leftmost Y-axes and individual Site Monitor push buttons along the uppermost X-axis. It visually displays activity data for the maximum number of channels found on each monitored site.

Text for primary and secondary assignments is displayed in white and black, respectively. A primary assignment is the site on which the call was originated. Secondary assignments are the other sites involved in the call.

NOTE: Confirmed and Forced calls may show multiple primary assignments.

For Multisite Monitor multinode traffic, outbound traffic from the node is displayed in a column representing the NIM, and inbound traffic to the node is displayed in a Device column. The MSM uses the Network Number to determine whichIMC, CEC, and Remote CEC to display columns for.

The level of detail is limited. (For maximum call information, use the Site Monitor instead.) By default, the column headings are of the form Site X and Device X. These may be modified in the configuration file as described in LBI-39171.

The main menu bar located at the top of the window contains three entries (refer to Figure 32):

- File

- Options

- Help.

The File menu has only one option: Exit. The Exit button terminates the MSM application.

Figure 31 - Multisite Monitor Display Example

The Options menu has four options: Traffic Filter, Legend, Statistics Rows, and Quiet Drops. The Options menu is discussed in the next section. These options allow the user to customize the Multisite Monitor application to suit particular needs

The Help menu also contains only one option: Overview. The Overview button provides a single help box documenting the overall functionality of the MSM application. Refer to the diagram below.

These menu options may be selected via the mouse or keyboard mnemonics.

12.1.1 Filtering Call Traffic

The Traffic Filter button activates a separate filter window as depicted in Figure 33. The filter window is also a row-column matrix layout with filter types listed in the leftmost column, followed by columns for filter state (On/Off), filter color, and filter text. Within this menu option, the user is allowed to modify the traffic filter on/off states, filter colors, and filter text settings for each EDACS traffic filter listed.   There are nine EDACS channel activity filter types: Emergency (EM), Individual (IN), Group (GR), Individual Data (ID), Group Data (GD), Individual to Telephone (IT), Telephone to Individual (TI), Telephone to Group (TG), and Control Channel (CC).

Each filter contains an On/Off switch to control filtering. The default is On for all filter types. When the filter is On, each time an event of this filter type is received, the channel button corresponding to the channel where the event is occurring is modified in color and text as defined by the user for that event type. If the filter is Off, channel activity of that filter type is not sent to the screen.

Each filter type has a color designation. There are 28 color options. Only one may be in effect at a time for a particular call type. The user's color choice sets the background color for each channel button currently processing an event whose associated filter type is on. The color defaults for each filter type are provided at startup. The color option choices are identical to those given by HP's ***xnmgraph*** utility, which is used to graph performance parameters in 2D line graphs.
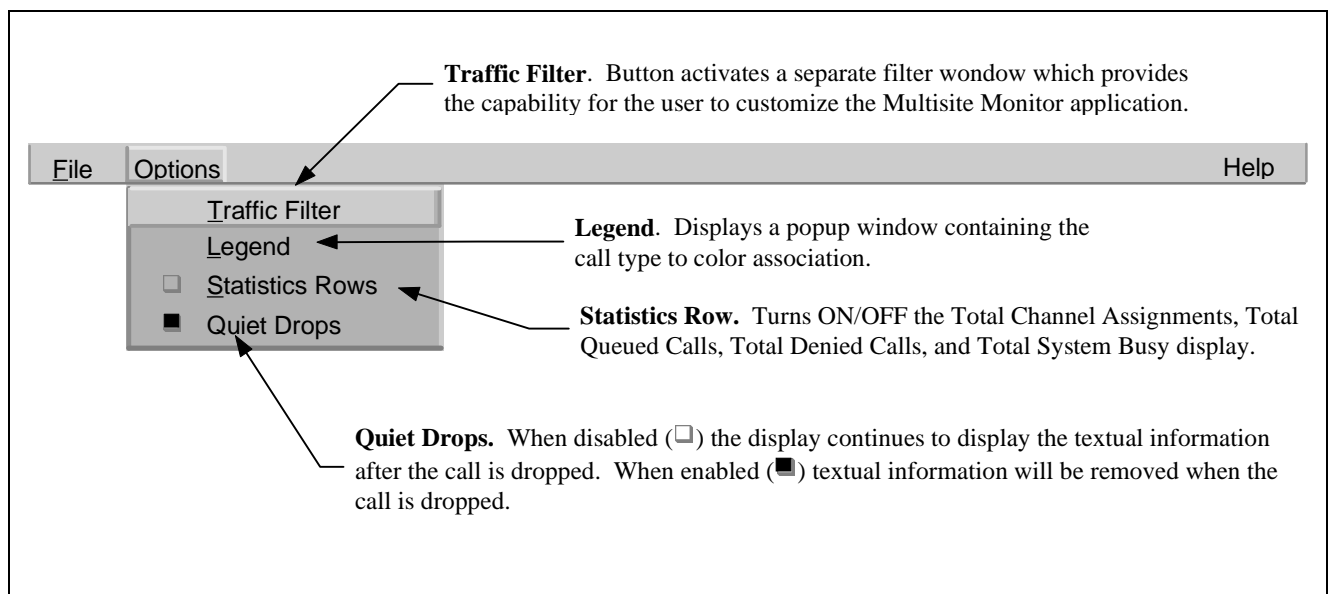
Figure 32 - Multisite Monitor Menu Bar

Each filter type also has a textual setting. There are five textual options. Only one may be in effect at a time for a specific call type.

1. None   No textual information is displayed.

2. Filter ID   One- or two-letter default designation for filter type (Example: EM, IN, GR, ID, GD, IT, TI, TG, CC).

3. Caller ID   Logical identification (LID) of caller.

4. Callee ID   Logical/Group identification (LID/GID) of callee.

5. Both IDs   Logical/Group identifications (LIDs/GIDs) of both caller and callee.

The Control Channel filter has only two of these options: None and Filter ID.

User-defined settings are not saved external to the application; therefore, the default settings are used upon MSM startup.
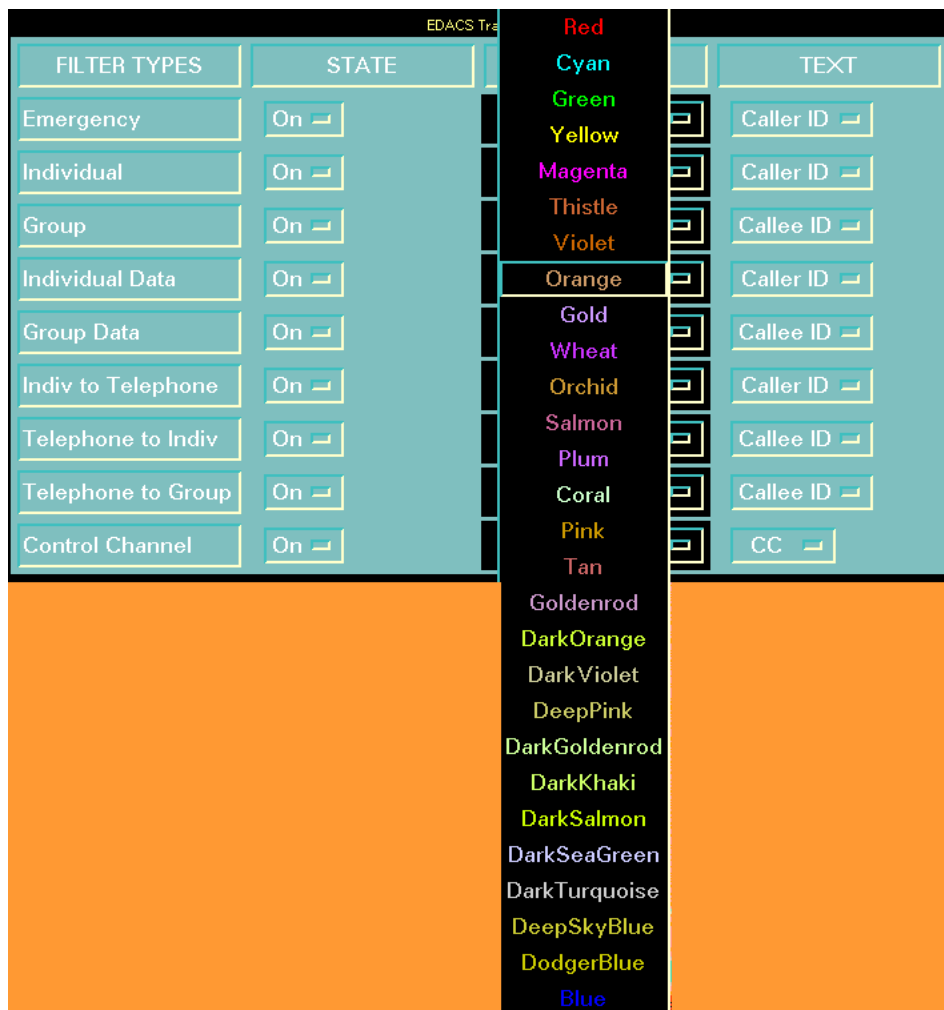
Figure 33 - Traffic Filter Window

12.1.2 Viewing Call Type Colors

The Legend button activates a small window that serves as a key for the current Traffic Filter settings (see Figure 34). Beside each filter is a button that conveys the filter's current state, color, and textual settings. If the filter state is Off, the button is black and states "Off." If the filter state is On, the button color is set to the chosen filter color and the button text is set to the chosen filter text. No modifications can be made to the filter settings via the Legend window. The window is for informational purposes only.

12.1.3 Displaying Site Statistics Rows

The Statistics Rows toggle button (default is On) forces the site statistics rows to appear/disappear from the MSM main window. The Statistics Rows are located along the bottom of the MSM window. There are four different rows: Assigned, Queued, Denied, and System Busy. There is a box for each statistic under every monitored site. The Assigned box maintains a counter of all call assignments for a particular site. The other boxes maintain counters for queued calls, denied calls, and system busy calls. The counters begin at zero (0) when the MSM application is invoked. Use the toggle button on the Options menu to view statistics rows or remove them from the main window.

Figure 34 - Multisite Monitor Legend

12.1.4 Indicating Quiet Drops

The Quiet Drops button, which defaults to "Off," displays textual information for a call in a channel button on the screen even after the call has dropped (color is removed). When Quiet Drops are turned "On" via the Options menu, both call color and text are removed from a channel button on the screen when the call is dropped.

12.2 USING THE SITE MONITOR APPLICATION

The Site Monitor application monitors call activity for an individual site. The Site Monitor window contains a main menu bar, work area, and scroll bars (see Figure 35). All windows can be manipulated (i.e., resized, iconized, closed) via standard window border operations.

The work area portion of the screen is arranged in a tabular format with channel numbers along the rightmost Y-axis. It displays activity data for specified channels. The activity data include channel number, current channel status (busy/free), time the call was initiated/dropped/keyed, caller ID, callee ID, call type, and phone digits (optional). Names of the caller and callee are not displayed. Primary and secondary assignments are shown.

A primary assignment is the site on which the call was originated, and secondary assignments are the other sites involved in the call. For primary assignments, text is displayed in white. For secondary assignments, text for the entire row except channel number is displayed in black. The title bar for the window may be modified in the configuration file as described in LBI-39171.

Scroll bars are generated automatically, as needed, for the work area.

The main menu bar located at the top of the window contains three entries (refer to Figure 36):

- File

- Options

- Help.

The File menu has only one option: Exit. The Exit button terminates the Site Monitor application.

The Options menu contains five options: Statistics Rows, Phone Digits, Fine Timing, Quiet Drops, and Keying Updates. These options allow the user to customize the Site Monitor application to suit particular needs.

The Help menu also has only one option: Overview. The Overview button provides a single help box documenting the function of the Site Monitor application.

These menu options may be selected via the mouse or keyboard mnemonics.

Figure 35 - Site Monitor Display Example
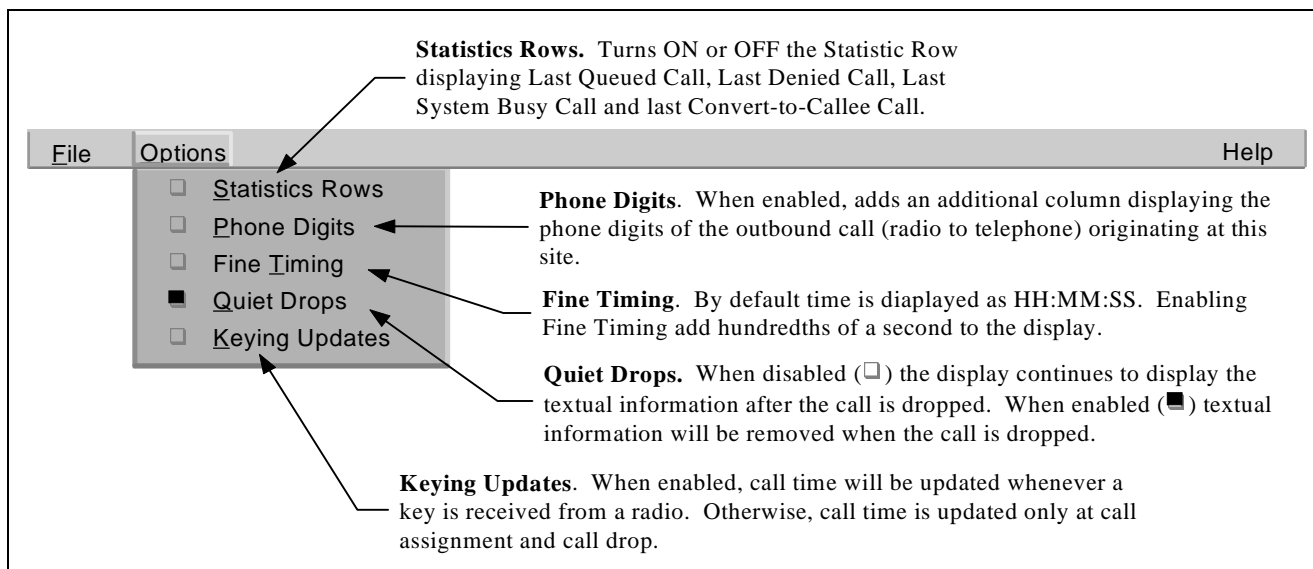
Figure 36 - Site Monitor Menu Bar

12.2.1 Turning On Statistics Rows

The Statistics Rows toggle button (default is On) forces the call statistics rows to appear/disappear from the bottom of the Site Monitor main window. There are four different rows: Queued, Denied, System Busy, and Convert to Callee. There is one row for each statistic. Each statistic row displays call information (i.e., Time, Caller, Callee, Call Type) for the last call that was queued, denied, system busy, or convert to callee. The information for these rows is blank at startup. Use the toggle button on the Options menu to view statistics rows or remove them from the main window.

12.2.2 Adding The Phone Digits Column

The Phone Digits toggle button forces the phone digits column to appear/disappear from the Site Monitor main window. The Phone Digits button, which defaults to "Off," does not display the Phone Digits column on the main window of the screen. When the Phone Digits option is turned "On," the phone digits column appears on the screen for displaying the telephone digits dialed by the caller. Phone digits will be displayed for radio-originated calls on the site of origination.

12.2.3 Setting The Time Fields

The Fine Timing toggle button forces the time fields to either seconds or milliseconds. The Fine Timing button, which defaults to "Off," displays call time in hour:minute:second format. When Fine Timing is turned "On," call time is displayed in hour:minute:second:millisecond format.

12.2.4 Enabling Quiet Drops

The Quiet Drops button, which defaults to "Off," displays textual information for a call in a channel button on the screen even after the call has dropped. When Quiet Drops are turned "On" via the Options menu, text is removed from a channel button on the screen when the call is dropped.

12.2.5 Changing Phone Call Keying Update Parameters

The Keying Updates toggle button forces radio keying to update/unaffect the time field displayed for a phone call. The Keying Updates button, which defaults to "Off," updates call time only at call assignment and call drop. When Keying Updates is turned "On," radio keys and unkeys update the call time for telephone calls.

13. USING OPENVIEW NETWORK NODE MANAGER

This section briefly describes some of the features available through OpenView Network Node Manager. We suggest the you become familiar with the **HP OpenView Network Node Manager User's Guide.** This guide contains detailed instructions for performing the task listed. The Network Manager application leverages the OpenView Network Node Manager to the fullest extent to achieve maximum similarity between our application and the customer's other OpenView Network Node Manager applications. Refer to the OpenView Network Node Manager documentation for a complete listing of features.

13.1 LOADING/UNLOADING MIBS

OpenView provides the mechanism to load/unload MIBs via the Options->Load/Unload MIBs main menu selection. By default, the EDACS MIBs are automatically loaded into OpenView.

13.2 VIEWING/GRAPHING PERFORMANCE PARAMETERS

NOTE

MIBs must be loaded to perform these operations.

Several menu selections are provided to graph the EDACS MIB items thought to be of most common interest via the EDACS -> Performance menu bar. However, numerous additional MIB variables are available. See the OpenView NNM User's Guide sections titled *Viewing MIB Values* and *Setting MIB Values* for procedures on using the MIB Browser to read and write MIB values. The MIB Browser provides the capability to graph individual MIB objects.

13.3 ADDING CUSTOM MENU ITEMS

Custom menus are realized using OpenView Network Node Manager's MIB Application Builder. The MIB Application Builder enables the easy development (without programming) of MIB applications for Internet-standard and enterprise-specific (i.e., specific to a given vendor) MIB objects, and integration of the applications into the HP OpenView Network Node Manager Windows menu bar. The custom menu item created may involve submenu items; therefore, all the user's custom-built additions may exist under one main menu bar item.

For custom selection, the MIBs Application Builder provides a list of the available performance values for the selected object(s) available for display via a menu item. Each performance value in the list contains the actual SNMP MIB variable name, its object ID, and a short description. The user may select one or more values from this list to monitor. Items for a custom selection must be from the same MIB, and all instances of the object are selected.

This feature is useful for MIB variables of interest on a periodic basis. Custom menu items may be built to view the MIB values. OpenView Network Node Manager has a MIB Application Builder to make this task relatively easy. See the OpenView NNM User's Guide section titled *Building MIB Applications*.

NOTE

The MIB Application Builder allows data to be displayed in form, table, or graph format, but does not allow the modification of MIB data. The MIB Browser is used to modify MIB data.

13.4 COLLECTING AND GRAPHING PERFORMANCE DATA

Data may be collected at regular intervals and saved to the **/usr/OV/database/snmpCollect** directory. The data are readable by **xnmgraph**. Note that performance data may be saved without graphing. If a graph is later invoked via the MIB browser, all of the previously collected data will be read in to xnmgraph and may be scrolled. See the OpenView NNM User's Guide section titled *Collecting MIB Data*.

13.5 THRESHOLD TRAPS ON COLLECTED DATA

The user may specify the generation of an event based upon the value of a monitored performance parameter or that parameter's exceeding a user-defined threshold. For example, the user may wish to be notified via a popup message (or e-mail) if the percentage of queued calls on a site reaches a certain value or goes above a specified threshold. This may be accomplished by selecting Options -> Data Collection.

When a collected MIB value exceeds a threshold value, a trap is generated. A rearm mechanism exists to avoid continuously generating events. This feature is a subset of the Collecting MIB Data feature. See OpenView NNM User's Guide sections titled *Collecting MIB Data* and *Defining Thresholds*.

13.6 VIEWING HISTORICAL TRENDS

Collected MIB data may be graphed later. The graph tool provided with OpenView Network Node Manager also allows the user to manipulate the data. See the OpenView NNM User's Guide section titled *Viewing Historical Trends*.

13.7 EVENT HISTORY

The OpenView Network Node Manager Event Browser can generate a report listing the past and present events. The Event Browser updates in real time, i.e., incoming alarms associated with that object or its children are immediately updated to the display. The report consists of entries describing the event source, time of occurrence, severity level, and type. The user may filter the event history report based upon the source, severity level, a specified time range, and/or event type. Any generated report can be saved to a user-specified file, and/or may be output to the printer. The Event Browser is automatically opened when OpenView comes up. It may also be invoked from Monitor->Events: SNMP. All received event entries that have been configured to be logged are written to a single file on the hard drive.

13.8 CUSTOMIZING EVENT MESSAGES AND ACTIONS

The event log message may be modified. In addition, the user may add his own specific text to the event comment field. The criticality level and category of the event may also be changed. In addition to affecting icon color, actions may be associated with events, such as paging, audible notifications, or other executables. See the OpenView NNM User's Guide section titled *Defining Actions for Events*. **NOTE:** Updates of the EDACS application will overwrite the event description (connect) field.

In the following example a burst of short beeps is associated with an SNMP event:

1. From the OpenView menu bar, select the **Options->Event Configuration:SNMP** menu item.

2. Select the enterprise that the sources the event. For example, System Manager, IMC Manager, PI, etc.

3. Select the event of interest.

4. Click on the Modify button, OpenView will display the Modify Event dialog box as shown in Figure 37.

5. Enter the following UNIX command line in the "Command for Automatic Action (Option)" field:

```
        /usr/OV/contrib/NNM/ringBell/rin
gBell dontLog ""
```


Figure 37 - Modify Event Screen

The ringBell utility takes two arguements. The value of the auguments are insignificant as long as the format is correct.

ringBell <selectionName> <message in quotes>

The ringBell utility performs two actions. It sounds the bursts of beeps and it sends an SNMP event to this management station using the OpenView enterprise specific trap OV_Bell_Message. If the logging of the OV_Bell_Message is undesirable, the Event Configuration feature may be used to set the category for this trap to "don't log or display".

6. Click on OK to save the changes.

13.9 BACKGROUND GEOGRAPHICAL MAPS

HP OpenView Network Node Manager provides the capability to assign a CompuServe Graphic Interchange Format (GIF™) file or an X11 monochrome bitmap format (XBM) file as the background for network maps. OpenView Network Node Manager ships with the set of standard image files shown below. These images are the only maps that Ericsson provides. The installer is responsible for selecting the appropriate maps at installation time or purchasing any additional maps (in the form of GIF or XBM files) desired.

- all 50 U.S. states

- major Canadian provinces

- western hemisphere

- continents

- countries in Europe, Asia, and the Pacific

The images that are provided are simple outlines located in *usr/OV/backgrounds*.

When a background graphic is added, the graphic appears in the submap window. Symbols in the submap appear over the background graphic file. Users and applications can specify a background graphic for each submap.

13.10 MAP SNAPSHOTS

Creating a map snapshot preserves the state of the network at the moment the snapshot was created. Snapshots can be created, listed, opened, closed, deleted, and described. Snapshots can not replace the current map. Snapshots are intended for historical purposes, not restorative purposes. See the OpenView NNM User's Guide section titled *Taking Snapshots of the Map*.

NOTE

Snapshots may consume noticeable amounts of memory.

13.11 MULTIPLE EDACS NETWORK MANAGER SESSIONS

OpenView Network Node Manager supports multiple login sessions. Multiple sessions can be accomplished by using an X-Station or by using a PC running PC Xware.

Certain restrictions apply in situations where multiple users are logged in using OpenView Network Node Manager. The main restriction is that only one user gets full map read-write access. All other simultaneous users of OpenView NNM get read-only map access. See LBI-39171, EDACS Network Management Installation and Technical Reference Manual, for information on restricting write access to OpenView.

The read version of OpenView will see icon status updates and be able to perform the following operations:

- Event Configuration

- IPMAP polling

- Application Builder

- MIB Browser

- MIB loading/unloading.

The main ramification of this restriction is that a read-only map cannot be edited. The effect of this is that during a read-only OpenView Network Node Manager session, any changes in map topology are not reflected; i.e., any newly discovered IP Network Elements are not shown to the read-only user. However, this also means that the user may not move icon positions on maps or delete/add icons. The customer may therefore designate the write privilege for an administrator and the read-only privilege for general users.

The read-only user continues to see Network Element status changes through icon color changes. Also, a read-only user can still run management applications to monitor performance and change configuration on Network Elements.

Remote login is supported via an X-session from the remote device to the EDACS Network Manager. This is available over a LAN or via a terminal server with modem (using SLIP or PPP). Due to memory constraints, the maximum number of remote sessions available at one time is dependent on the EDACS Network Manager option chosen. Refer to the Remote Access section in the Installation manual, LBI-39171.

13.12 INTEGRATION WITH OTHER NETWORK MANAGER APPLICATIONS

OpenView Network Node Manager provides the mechanism for allowing multiple applications to be registered with it via Application Registration Files (ARFs). In order for the EDACS Network Manager to be interoperable with other OpenView Network Node Manager-based applications, all applications must be registered with OpenView Network Node Manager. The ARF provides information to OpenView Network Node Manager on how to integrate the application into the menu structure, how to invoke the application, and how to manage the application.

The EDACS menu co-exists with all other menus, including those added by another EDACS NM application. The user of the EDACS Network Manager can manually place icons from another application into EDACS NM maps or vice versa.

13.13 CUSTOMIZING ICONS

13.13.1 Icon Labels

――――――――――――――――――― **NOTE** ―――――――――――

Modifications to fields other than "Label" in the Symbol Description are not supported and may adversely affect system behavior.

To change icon labels, depress the right mouse button while positioned on the icon and select Describe/Modify Symbol. Enter the information in the "Label" field.

13.13.2 Object Descriptions

To add object descriptions to the underlying database, depress the right mouse button while positioned on the icon and select Describe/Modify Object. Enter the object description in the "Comments" field. The object description might include the name of the person responsible for the equipment, etc.

Note that if there are multiple icons associated with the database object, all symbols will have access to the description.

13.13.3 Icon Bitmaps

Icon bitmaps may be modified, but doing so is not recommended. HP-UX has an icon editor tool which may be used to easily tailor the bitmap. The **/usr/OV/symbols/C/EDACS** registration files provide the association of symbol to bitmap. Each bitmap is composed of a pixel and mask file. The pixel bitmap is new_bm.38.p and the mask bitmap is new_bm.38.m. If the EDACS bitmaps in **/usr/OV/bitmaps/C** are modified, they can be restored from **/usr/EDACS/bitmaps/C**. Bitmaps of sizes 38, 32, 28, and 20 are required to handle various sized icons which occur with window resizing.

13.14 LOADING MIBS

OpenView comes preloaded with RFC-1213 (MIB II) and HP-UNIX MIBs only. EDACS MIBs will be automatically loaded when the edacsInstall utility is run. Please refer to the "Loading MIBs" section in the HP OpenView Network Node Manager User's Guide for detailed information.

14. PROCEDURES

14.1 REBOOTING THE NETWORK MANAGER

From the *root* profile enter:

> **/etc/shutdown -r now**

14.2 SYSTEM SHUTDOWN PROCEDURES

Use the following procedure to properly shutdown the Network Manager system.

```
CAUTION
```

Stopping the system improperly can corrupt (damage) the file systems. Never stop the system by turning it off.

1. Log out of all software applications. You should be at the log-in prompt. If you have a VUE Login prompt, select Options -> No Windows.

2. Change to the root directory.

    > **cd /** *<ENTER>*

3. Ensure no one else is logged in by entering the following command:

    > **users** *<ENTER>*

    Ensure no other users, other than yourself, are listed on the display.

4. At the prompt enter the shutdown command:

    > **/etc/shutdown -h** *<ENTER>*

5. Watch the messages during the process and note actions.

    The system is completely shutdown when the system displays "**HALTED**" and pressing a key has no effect.

6. After the system has halted, it is safe to turn off the equipment, starting with the computer/server.

14.3 DEVICE POLLING INTERVAL

The EDACS Network Manager Application may be initialized for the interval between polls for missed events detection and for the Node to which the EDACS Network Manager application should synchronize the clock.

The device polling interval is defined as the time (in seconds) between polls of each device. A device is considered to be any of the following:

- Integrated Multisite and Console Controller (IMC)

- Console Electronics Controller (CEC)

- StarGate Controller

- IMC Manager

- System Manager

- Console

- Jessica PBX Interface (PI)

- Billing Correlation Unit/ Centralized Activity Logger (BCU/CAL)

NOTE: The site devices are not included in this list. Their status is obtained through the System Manager Proxy Agent.

The EDACS Initialization attribute section of the popup associated with the "EDACS Top Icon" Describe/Modify operation specifies the clock and device polling intervals.

14.3.1 Polling Interval Setup

The number of polls per device varies depending upon the device. In addition, some devices have summary status capability. If the summary indicates an active trap, further polling is enacted to determine which conditions are active.

To determine the frequency by which an individual device is polled, one must multiply the interval by the number of polled devices in the EDACS network.

The following equation may be used to determine the time between successive polls of the same device:

$$\frac{\text{Device Polling Interval(s)}}{\text{Device}} \times \text{Devices} = \text{Time between Device Successive Poll(s)}$$

By default, status polling is disabled. The device polling interval is associated with the EDACS top container icon.

Polling parameters associated with EDACS Top level Icon (looks like a world globe) can be modified on icon add or modified using procedure to describe EDACS identifiers.

NOTE

We strongly recommend setting the polling interval to a value of 30 seconds or more. If the interval level is set below this value, and multiple Network Manager stations are polling the System Manager, there may be an increase in the number of SNMP "sets" failures. This results from the frequency of polling requests exceeding the System Manager's response time.

14.3.2 Clock Synchronization

The Node Number of the CEC/IMC Manager is set to act as clock synchronization source. The default is that the Network Manager will not synchronize to any Node.

14.3.3 Clock Polling Interval

The clock polling interval is defined as the time (in minutes) between successive polls.

14.4 MODIFYING EVENT DESCRIPTIONS

1. From the OpenView Menu bar, select Options->Event Configuration: SNMP.

2. Select the enterprise that sources the event. For example, Sysman, IMCMan,etc.

3. Select the event of interest.

4. Click on the Modify button.

5. Click **OK** to save the changes.

14.5 ADDING SYMBOLS TO EDACS MAPS

Use the following procedure to add symbols to the EDACS Maps.

To drag a symbol onto an OpenView Network Node Manager Map,

1. Select the **EDIT-> Add Object** Menu item from the OpenView Network Node Manager main menu bar. An Add Object Palette window appears.

2. Scroll through the Symbol Classes until the EDACS class appears.

3. Double click on the EDACS Symbol class and the individual EDACS symbols appear.

4. Position the mouse over the symbol of interest, press the middle mouse button, and drag the symbol onto the desired map.

5. Depress the mouse, and the popup window appears.

6. Select the "EDACS Map Generation" attribute section and "Set Object Attributes." Fill in the identifiers and any other applicable fields. The Help button provides on-line help to for field meanings.

7. Follow the on-line OpenView NNM help to fill in the remaining window fields.

8. Notably, the selection name specifies the database key for the object represented by the symbol. Therefore, the selection name must be unique for all objects. The one exception is the selection name for directly connected EDACS elements - BCU/CAL, PI, EDG, System Manager, and CEC/IMC Manager. Directly connected elements must have their selection name equal to the one found by IPMAP. IPMAP will use the host name by preference but will use the IP Address if it cannot determine the Host Name.

After the symbol is added, it may need to be connected to another symbol using the Adding a Connection procedure, which is presented below.

14.6 DELETING SYMBOLS

Use the following procedure to delete a symbol from the OpenView map.

1. Select the symbol with the left mouse button.

2. Select the **EDIT->Delete->From All Submaps** menu item from the OpenView main menu bar.

    A Delete Object warning popup will appear.

NOTE

To delete a symbol that has a submap, select **EDIT->Delete->From All Submaps**. Selecting **EDIT->Delete->From this Submap** to delete a symbol will cause the symbols on the submap to be orphaned and remain in the OpenView database. To access orphaned submaps, do **Edit->Submap** which will list all submaps, then perform the *Deleting Orphaned Submaps* procedure.

14.7 ADDING A CONNECTION

When an EDACS icon is manually added for a directly connected EDACS element, the selection name must equal the IP Address of the element. The following elements are directly connected EDACS elements: PI, BCU/CAL, CEC/IMC Manager, and System Manager. This ties the EDACS icon with the EDACS capabilities to the object created by IPMAP, the

HP application which finds IPs. It is also possible that directly connected elements may be added prior to their discovery by the IPMAP application. Care must be taken to ensure that the object created is also used by IPMAP. Not only must the selection name equal the IP address, but the IP Host Name must equal the Host Name that IPMAP will find. Note that by associating the EDACS icon with the same object defined by the IPMAP application, the directly connected element will have a child submap containing icons representing the interfaces defined in MIB-II (i.e., the IP interface group will have an icon). The parent of this child submap is in the IPMAP screens, not the EDACS-created screen.   This feature can aide in network connection debugging. Namely, to see where this element is in the overall network, enter the IP child map and select the "parent" button.

Use the following procedure to add a connection between two symbols on an OpenView map

1. Select the **EDIT->Add Connection** menu item from the OpenView main menu bar. An Add Connection window will appear.

2. Select the representation for the connection type by clicking on the representation with the left mouse button.

3. The Add Object window appears.

4. Select the source symbol.

5. Select the destination symbol.

14.8 CUSTOMIZING MSM/SM SITE/DEVICE LABELS

Use the following procedure to customize the site or device labels.

1. As *root* user perform the following:

    > **cd /usr/EDACS/nls/C   *<ENTER>***

2. Edit the MSM message file, **/usr/EDACS/nls/C/msm_msg.msg** or the SM message file, **/usr/EDACS/nls/C/sm_msg.msg,** to reflect the new label(s).

    > **chmod 777 /usr/EDACS/nls/C/msm_msg.msg   *<ENTER>***   (MSM message file)

            or

    > **chmod 777 /usr/EDACS/nls/C/sm_msg.msg   *<ENTER>***   (SM message file)

3. Invoke the vuepad and edit the files as required. See the following examples.

    For example, if you want to change the label for site 1 from "Site 1" to "Candlers" change the line for site 1 as follows:

    As reads: **25014   "Site 1" Site_1_label**

    Change to read: **25014   "Candlers" Site_1_label**

NOTE

There is only one Site X label. Modification of the Site X label will be reflected in all nodes. Remember, Site labels may be up to eight (8) characters long and Device labels may be up to ten (10) characters long.

To change a device label for site 1 from "Device 33" to read "Dallas" change the line as follows:

    As reads: **15021   "Device 33" Device_33_label**

    Change to read: **15021   "Dallas" Device_33_label**

4. Enter the following command to restore permissions.

    > **chmod 444 /usr/EDACS/nls/C/msm_msg.msg** *<ENTER>*   (MSM message file)

           or

    > **chmod 444 /usr/EDACS/nls/C/sm_msg.msg** *<ENTER>*   (SM message file)

5. As the *root* user, generate new catalog files by executing the following :

           > **/usr/EDACS/bin/edacsMsgUpdate**

6. Test changes by invoking MSM and SM.

14.9 ADDING DESCRIPTIONS TO OBJECTS

This procedure requires you to be logged into a write version of OpenView.

1. Position the mouse over the desired icon and depress the right button.

2. Select the "Describe Modify Object"

3. Make desired changes or add text to the "comment" field.

NOTE

Changing the "Selection Name" is <u>not</u> recommended. The Selection Name is used as the database key.

---

4. Select **OK** when done.

14.10 DELETING ORPHANED SUBMAPS

This procedure describe the process for deleting orphaned submaps for OpenView.

1. From the OpenView menu, select Edit -> Submap ->OPen/List...

2. A "Submaps in Map" popup with Submaps scroll box will appear.

3. Select the submap believed orphaned and click on the "Open Submap" button to bring up the submap.

4. On the opened submap, click on the "Parent" button to verify there is no parent map.

5. Ensure the orphaned submap is highlighted, go to the "Submaps in Map" dialog box and click on the Delete button. The submap will be deleted.

14.11 VERIFYING AN OBJECT WAS DELETED FROM THE OPENVIEW DATABASE

Selecting an explodable icon and selecting EDIT->Delete->From this Submap rather than EDIT->Delete->From all Submaps can orphan objects in the OpenView database which affects the performance of the system. To determine if a file contains orphaned objects, perform the following:

1. Enter:

       > **/usr/OV/bin/ovobjprint |more.**

The beginning of this output will list the number of objects in the database. There should be roughly three times the number of EDACS elements.

2. Enter:

> **/usr/OV/bin/ovobjprint >** *Filename*

This will output the contents to a file called "Filename."

3. The individual objects can be viewed in "Filename."

14.12 VIEWING/MODIFYING EDACS IDENTIFIERS

To view/Modify that the EDACS identifiers are correctly associated with an icon, perform the following:

1. Select the icon using the left mouse button, and then select the **Monitor ->Description->Selected Object** menu item from the OpenView main menu bar.

2. Choose the EDACS Identifiers attributes. The identifiers will be listed.

3. Press the View/Modify Object Attributes button.

OR

1. Select the icon, depress and hold down the right mouse button.

2. Move the mouse to the Describe/Modify Object...menu option and release the mouse button.

3. Select the EDACS Identifiers Object Attributes and press the View/Modify Object Attributes button.

14.13 VIEWING/MODIFYING TRAP SEVERITY LEVELS

Use the following procedure to view or modify trap severity levels.

1. Select the **EDACS->Faults->Configuration** menu item to invoke the OpenView event configuration.

2. Select the enterprise of the agent reporting the traps, and the traps defined for the agent will be displayed in the middle window. The severity level will be displayed in the middle window along with the trap name. The first characters of an EDACS trap name conventionally are an acronym of the device against which the trap is placed.

3. Select the event which has the severity level to change and choose the Modify button. A new window will pop up with the severity levels in the lower right-hand corner.

4. Click on the severity button and a pulldown menu will display choices.

5. Select the **OK** button to exit this popup and click on the **Apply** button on the Event Configuration window for the changes to take effect.

14.14 MODIFYING EVENT DESCRIPTIONS

To modify the event descriptions you must bring up the OpenView Event Configuration application.

1. Select **EDACS->Fault->Configuration** from the EDACS menu bar.

2. Select the enterprise of the agent reporting the traps, and the traps defined for the agent will be displayed in the middle window. The severity level will be displayed in the middle window along with the trap name. The first characters of an EDACS trap name conventionally are an acronym of the device against which the trap is placed.

3. Click on the Modify button and a window will popup.

4. Modify the text as required. **NOTE:** Modifications will be overwritten when the application is upgraded.

5. Select the **OK** button to exit this popup and click on the **Apply** button on the Event Configuration window for the changes to take effect.

14.15 RESTORING DEFAULT EVENT DESCRIPTIONS

To restore the default event descriptions execute the following command:

```
> /usr/OV/bin/xnmevents -load /usr/EDACS/conf/C/ed_trapd.conf
```

14.16 MAPPING SEVERITY LEVEL TO ICON COLOR

1. Select **Help->Display Legend** from the OpenView main menu bar, this will provide a graphical display of the icons and their associated colors.

14.17 CREATING A FULL SYSTEM IMAGE BACKUP

To create a full system image backup, perform the following steps:

1. As *root* user: Use console login.

   ```
   > /etc/shutdown now   <ENTER>
   ```

   System will shutdown and come back up in single-user mode. If asked what terminal type, press **<Enter>**

2. Insert the tape into the tape drive (assume device name = /dev/rmt/0m).

   ```
   > cd /  <ENTER>
   ```

   ```
   > tar -cvf /dev/rmt/0m .  <ENTER>
   ```

NOTE

One 90mm tape should handle the entire backup and the backup process will take approximately one hour to complete.

When the backup is complete, carefully label all System Image backup tapes as "Sys*ddmmmyyyy* Vol # *(number of this tape)* of # *(total number of tapes it took to complete the backup)*".

For example: Sys12DEC1994 Vol 1 of 4.

---

3. Enter the following command to reboot the workstation.

   ```
   > /etc/shutdown -r now   <ENTER>
   ```

14.18 RESTORING A FULL SYSTEM IMAGE FROM THE BACKUP

To restore a full system image from the backup, perform the following steps:

1. As *root* user: Use console login.

    > **/etc/shutdown now** *<ENTER>*

    System will shutdown and come back up in single-user mode.

2. Insert the tape into the tape drive (assume device name = /dev/rmt/0m).

    > **cd /** *<ENTER>*

    > **tar -xvf /dev/rmt/0m .** *<ENTER>*

3. Reboot the workstation as shown below.

    > **/etc/shutdown -r now** *<ENTER>*

15. TROUBLESHOOTING

This section presents various methods for solving technical difficulties with the Network Manager.

15.1 CD-ROM DOES NOT WORK

Problem: */etc/update* exits with error that all devices are not mounted.

Solution:

The */etc/checklist* file should have only list the hard drives. The Tape Drive and CD-ROM drive should not be listed in it. If peripherals are listed in this file, then updates will not work.

Procedure to access CD-ROM:

The CD-ROM is mounted when there is a disk in it using the `mount /dev/dsk/c201d2s0 /cdrom` command. Once mounted, the */cdrom* directory is accessed like any other directory. The disk cannot be removed until an `umount /dev/dsk/c201d2s0` command is performed.

15.2 MSM/SM DOES NOT SHOW PI TRAFFIC

Problem: MSM/SM does not show PI traffic, but shows Group and ICall traffic.

Solution:

Do `traf -e -sX` on the PI or `stat -e -sX` on the BCU/CAL where X is the PI Site_Id. If is shows that the packets the PI received were errored with Null Caller ID then check the Line database definition for the PI site in the System Manager. If the Line is enabled and the LID is 0, this is invalid and causes this problem. If there is only one PI in the Network all lines should be N. In a multinode PI configuration, the Line database must have a unique LID assigned for each PI line. See LBI 39000A.

15.3 ATTEMPT TO LOG IN FAILS

Problem:

When the disk fills up, the following situations occur:

- All users who attempt to log in will be in the *root* directory (/).

- None of the user's initialization files will be executed, i.e., the environment variables (such as $path) may not be set correctly, and the general appearance of the screen will seem unusual.

- Any process that tries to write to disk is likely to hang (this includes almost all processes).

- The message "Cannot write to file: disk system full" will appear at the bottom left corner of the screen at the console. If the user is not at the console, he may not see the error message. If a remote user notices odd behavior, he should check for error messages on the screen that is connected as the console.

Solution:

Most likely, the log files have grown too large. Delete the log files in */usr/EDACS/logs/***filename**. DO NOT ERASE *edacs.log*. Also, periodically check */usr/netls/log_file* and */usr/OV/log/trapd.log* and delete files as necessary.

15.4 EDACS ICON IS BLUE

Problem:

The EDACS icon is blue.

Solution:

A blue icon indicates that the element is not managed by the EDACS Network Manager application. This can happen if another icon is added with the same EDACS Identifiers as this one. To view the EDACS Identifiers, select the icon and press the right mouse button. Keep the right mouse button depressed and move the mouse to the Describe/Modify Object... menu item and release the mouse button. Select the EDACS Identifiers Object Attributes and press the View/Modify Object attributes button. To map severity level to icon color, select Help->Display Legend from the OpenView main menu bar to display the legend.

15.5 EDACS ICON IS BROWN

Problem:

The EDACS icon is brown.

Solution:

A brown icon indicated that the element is restricted. An icon is restricted if there is no licensed CEC, Remote CEC, IMC, or StarGate with the same Network Number and Node Number. An icon may also be restricted if it violated a CEC/RCEC/IMC/StarGate licensing node. An RCEC allows 0 sites, a CEC allows 1 site (maximum), an IMC allows >1 site, and a StarGate allows 0 sites.

15.6 RPC FAILURES

Problem:

Remote Procedure Calls are failing.

Solution:

The RPCs may be failing because the hostname for contacting the license server daemon is not defined. There are two options for defining the hostname. In one option, set the EDACS_LICENSE_SERVER variable by entering the following information at the UNIX prompt: *setenv EDACS_LICENSE_SERVER* **hostname**. If this variable is set, the client processes will use the defined hostname to contact the license server daemon. If the EDACS_LICENSE_SERVER variable is not set, then the second option for defining the hostname is assumed. In the second option, check the *localhost* variable in the */etc/hosts* table to ensure that the variable is defined. If the variable is not defined, enter 127.0.0.1 in the host table.

15.7 MAP GENERATION VERIFY OPERATION IS NOT WORKING PROPERLY

Problem:

The Map Generation Verify operation sometimes does not work on a Describe/Modify operation unless one of the parameters is changed.

Solution:

There is an OpenView anomaly which sometimes requires the user to modify one of the dialog box fields before the Verify button will accept identifier values. Whether the Verify button works depends on which icons are present on the map. If a CEC Node, an RCEC Node, and an IMC Node exist on the same map (with or without the same Network and Node Numbers), the first two of these three icons asked to perform a Describe/Modify operation will work properly. The Verify button for the third icon will not accept the identifiers values until one has been changed (or at least deleted and reentered).

15.8 POPUP STATES NO NODE LICENSE

Problem:

This popup will occur either if there is no node license or if there is no application license.

Solution:

Use ls_stat to determine if either of these conditions exist.

15.9 PERFORMANCE NOT SHOWING TRAFFIC

Problem:

No traffic indicated on MSM, SM, or 2D line graph.

Solution:

Traffic is as seen on by the IMC. Therefore, site only traffic such as denies and local interconnect will not be seen. If no traffic is seen the NM and BCU/CAL/PI may not be time synched. Log into the BCU/CAL. Do stat-e-sx, where x is a site tour radio is on. If bad time stamp is indicated, check source of MOM PC clock.

15.10 POOR SYSTEM PERFORMANCE

Problem:

System is slower than usual.

Solution:

1. IPMAP autodiscovery may be enabled. From the OpenView Main menu select Options -> Topology/Status Polling:IP and turn off the polling Master switch (raised button).

2. Do ps -ef | grep edacs

   Only one instance of each of the following three processes will be running an a NMS:

   root   196   186 0 Sep 16 ?   3:45 edacs_nm

   root   299   1 0 Sep 16 ?   0:00 /usr/EDACS/bin/edacslog

   root   301   1 0 Sep 16 ?   1:48 /usr/EDACS/bin/edacs_licservd

   There will be one instance of each of following three processes running for each user. If there are more processes than simultaneous users, a user could have improperly exited and left processes running with no UI attached.

   guest 20060 20059 0 07:10:44 ?   0:00 /usr/EDACS/bin/edacsd

   guest 20061 20059 0 07:10:44 ?   0:00 /usr/EDACS/bin/edacsi

   guest 20062 20059 0 07:10:44 ?   0:00 /usr/EDACS/bin/edacsm

15.11 APPLICATION DOES NOT RESPOND TO VERIFICATION REQUEST WHEN ADDING ICON

Problem:

Application does not respond to Verification request when adding icon. When hit verify a second time, OpenView will not call application again.

Solution:

Must modify a field, even if setting it to the same value, before OpenView will send request to the application again.

15.12 IFOR/LS CONFUSED

Problem:

When the IP address of an Network Manager box is modified after our application has been installed, IFOR/LS will be confused.

Solution:

Perform the following instructions to restore IFOR/LS to a working configuration (must be *root* user):

Be sure there are no other users on the system.

> **> users**

Stop OpenView, EDACS NM application, and IFOR/LS servers.

> **> /usr/OV/bin/ovstop**
> **> /usr/EDACS/bin/ks**
> **> /usr/lib/netls/bin/srv_stop**

3. Reconfigure IFOR/LS. (Reference the NM Installation LBI procedure.)

> **> cd /usr/lib/netls/conf**
> **> ./netls_config**

When prompted whether or not to use the existing global database found on the system - Answer NO. Answer all other questions as done during the initial installation.

NOTE

Reference the NM Installation LBI procedure for Licensing Run Time Kit Setup and Installation.

15.13 SYSTEM MANAGER SNMP "SETS" FAILING

Problem:

System Manager exhibits an increased number of SNMP "sets" failures when multiple Network Manager stations are polling the System Manager.

Solution:

The System Manager SNMP "sets" are used to control trap generation on the System Manager by setting its trap control objects. If multiple Network Managers are polling the System Manager with intervals of less than 30 seconds, the System Manager may be unable to keep up with the requests. Check the polling intervals on the

Network Manager stations and ensure the interval is set to a value of 30 seconds or more. This will significantly reduce the number of nuisance failures.

15.14 IMC DETECTED LINK FAILURES

Problem:

The IMC reports a link failure.

Solution:

For link fail tests involving all controller types (MIM, PIM, etc.), the steps below will help to identify the defective controller board.

- On the CEC/IMC Manager For NT, display the nodes map. All boards managed by this IMC should appear on the screen with the appropriate status icon. For example, to perform a MIM fail link trap test, click on the MIM icon. Another menu appears when the user selects the "controller" box and then "send." Next, go to the switch and determine which controller board's LED is flashing. This step is useful only when boards and cables are not properly tagged or labeled.

- After finding the correct board, go to the back of the switch and carefully pull the cable to that controller board. Within 10 seconds, the status of the appropriate controller board icon on the CEC/IMC Manager node map will change (turn red) and a trap should be received at the workstation where the Network Manager is running. The trap will appear as an EDACS event if it is correctly categorized as an EDACS event.

- If the trap is not received, make sure that the MIB object associated with the trap enable/disable is not set to "disable." If the MIB object is "enabled," then make sure that the trap is properly configured to be an EDACS event. To check this condition, enter the EDACS->Faults->Configuration menu.

15.15 MSM/SM OUT OF COLOR MAP ENTRIES

Problem:

The Multisite Monitor or Site monitor application errors out with one on the following X messages:

- Warning: Cannot allocate colormap entry for "xxxx". (Where xxxx is a color name.)

- Warning: Cannot parse default background color spec.

- X error of failed request: Bad Access (attempt to access private resource denied.)

- Major opcode of failed request: 88(X_FreeColors)

- Serial number of Failed request: stream: 16747

The X server will not recover from these errors and must be killed manually. It will restart automatically. NOTE: These errors should not occur if MSM or SM is started before the graphic intensive submaps are opened.

If the MSM is executed from the command line after the OpenView submaps have been opened, the MSM application will execute without "X" messages, but the colors are confused. The X-server does not need to be restarted is this case.

Solution:

This problem is results from all software colormap entries in use. The MSM must allocate approximately 30 color entries to execute. The 712 workstations have a maximum of 256 color entries, therefore only 256 different colors/shades can be displayed or used on the system at any given time. HP-VUE claims some of these color entries and the NNM claims another 128 entries. When color-intensive background maps are used on OpenView submaps, they also use up color entries in this software colormap.

The only viable solution is to refrain for using color-intensive background graphics in the OpenView submaps.

15.16 POPUP WARNING

Problem:

An xnmevent popup warns that only 10 popups can be generated at a time.

Solution:

The */usr/OV/appdefaults/XNm* resource file sets the **xnmevents.maxDisplayMsgs** to ten (10). This can be modified if desired. The limit is set to this value so all the system resources are not used up by popups when no one is around to clear them.

15.17 MULTINODE TRAFFIC NOT SEEN CORRECTLY ON MSM SESSIONS

Problem:

MultiSite Monitor fails to display originating node traffic on NIM (site) column and destination node traffic on Device (node) column.

Solution:

Sometimes the CEC/IMC CAM card gets confused, especially if it has been moved between card cages. To clear the problem, clear the CAM's NOV RAM using the following procedure (For CEC/IMC information, refer to LBI-38938):

1. Remove the CAM card and reset the DIP switches so the card will function as another device, such as a CIM.

2. Reinsert the card into the card cage. This will clear the NOV RAM.

3. Remove the card and reconfigure the DIP swiches so card card will function as a CAM.

4. Reinsert the card.

16. GLOSSARY

<u>**TERM**</u>   <u>**DEFINITION**</u>

ACU   **A**larm and **C**ontrol **U**nit. The ACU provides 32 alarm inputs and 8 relay outputs and allows for external device alarming to the System Manager. The ACU and Test Unit (TU) form the Test and Alarm Unit (TAU).

Administrator (or Admin or   Administrators are those people responsible for centralized configuration of
EDACS Administrator)   EDACS networks. Their role is to install and maintain the system-wide database, and in the case of Network Management, overview the operation of the network.

Aegis™   **Aegis™** is the Ericsson GE's voice scrambling system that employs advanced Digital Signal Processing (DSP) circuitry. Aegis has two primary modes − "Aegis digital" and "Aegis private". Aegis digital mode offers improved weak signal performance and impedance to unauthorized monitoring. Aegis digital transmissions <u>are not</u> encrypted. Aegis private mode also offers improved weak signal performance. In addition, since Aegis private transmissions <u>are</u> encrypted, Aegis private mode provides very secure communications against unauthorized monitoring.

Agent   Software that enables a device to respond to manager requests to view or update MIB data, and send traps reporting problems to significant events.

AMTS   **A**dvanced **M**ultisite **T**est **S**ystem.

API   **A**pplication **P**rogramming **I**nterface. Standard interface to a software application.

Audio Board   The **Audio Board** routes audio, mobile data and Aegis data between EDACS radio systems, dispatch consoles, logging recorders, etc. The board digitizes analog signals applied to its audio inputs and applies the digitized signals to the TDM bus. It also performs the reverse process for its audio outputs.

AUI   **A**ttachment **U**nit **I**nterface. Connector used with thick Ethernet that often includes a drop cable.

Battery-backup   Holds information in RAM until power is restored or battery is drained.

BCU   EDACS **B**illing **C**orrelation **U**nit. This EDACS unit converts Integrated Multisite Controller activity to Call Detail Records which can be used for billing.

Bridge   Used to connect Ethernet to Ethernet with capability to control two-way traffic. OSI data Link and Physical layers only.

C3 Maestro   The **C3 Maestro** is the CRT-type console that is designed to take advantage of the advanced features of EDACS. It consists of a specialized audio "tower" and an IBM PC compatible computer running custom software developed by Ericsson GE.

CAL   **C**entralized **A**ctivity **L**ogger. This EDACS unit is inserted between the IMC and the System Manager to provide activity information from Basic EDACS,

TERM	DEFINITION
	SCAT, and CNI systems.
Callee	The party to whom the call is placed, i.e., an individual or group of radios.
Caller	The originating party of the call request, i.e., an individual radio.
CAM	**C**entralized **A**ctivity **M**odule − The CAM is a CEC/IMC interface module that provides call activity information to the **C**entralized **A**ctivity **L**ogger (**CAL**) computer. Usage and billing information can be generated with the CAL through the CAM link.
CAP	EDG **C**entral **A**ctivity **P**rocessor. Provides an IP Ethernet interface to host computers and system services such as disk I/O, printing, and the Local Diagnostic Terminal interface.
CCI Board	**C**onventional **C**ontrol **I**nterface **Board** − This is a CEC/IMC Controller Board configured for use in the CIA rack. It provides master CI Board control. The control data port that connects the CIA rack to the VMIM is also located on the CCI Board. (Also see **CI Board.**)
CCITT	**C**onsultative **C**ommittee on **I**nternational **T**elephony and **T**elegraphy. An international organization which sets standards for interconnection of telephone equipment.
CD-ROM	**C**ompact **D**isk **R**ead **O**nly **M**emory. A media used for software and information distribution.
CEC	**C**onsole **E**lectronics **C**ontroller − The Ericsson GE CEC is an advanced radio communications controller incorporating time division multiplex digital audio switching technology. The CEC connects dispatch consoles to EDACS and CNI systems.
CEC Node Icon	A CEC Node icon consists of a CEC, Console(s), and the Site(s).
CEC/IMC Manager	The **CEC/IMC Manager** (formerly referred to as the "MOM PC") provides CEC/IMC switch monitoring and configuration functions. This IBM PC compatible computer running custom software developed by Ericsson GE is the window into the CEC/IMC switch for the system administrator and service technicians.
Channel	The smallest division of a frequency band which provides a single communication circuit, such as a voice or data channel.
CI Board	**C**onventional **I**nterface **Board** − This board is located in the CIA secondary interface rack. It contains circuitry used to connect conventional tone and dc controlled base stations and voting systems to the CEC/IMC switch.
CIM	**C**onsole **I**nterface **M**odule − The CIM is a CEC/IMC interface module used to connect C3 Maestro (CRT-type) and C3 Modular/Desktop consoles to the CEC/IMC switch. C3 Modular/Desktop consoles also require a C3 Console Translator interface module. (Also see **XLTR.)**

<u>**TERM**</u>	<u>**DEFINITION**</u>
CNI	**C**onventional **N**etwork **I**nterface − A conventional base station can be connected to the CEC/IMC switch via a CNI. The CNI is formed by a GETC shelf located at the conventional station that makes the station appear to a MIM as an EDACS site. In the CNI system, different Channel Guard tones are assigned to different talk groups.
Community Name	Used like a password in message, validating the right of the sender to access MIB data with a requested operation.
confirmed call	The **confirmed call** function ensures all EDACS radio systems being called have working channels available before the caller is given a channel access (talk permit) tone. This function can be disabled on a per system/group basis.
Console	Communication equipment which provides an operating position for a dispatcher.
Console Icon	The Console icon consists of equipment, displays, and controls where one operator interfaces with a radio system.
Convert To Callee	The convert to callee message is sent to a radio which attempts to initiate a call within a group which is already assigned a working channel. Upon recept of the message, the radio is prevented from transmitting and is placed in the receive mode on the assigned working channel.
control data	**Control data** includes any data used by the switch for system control.
CTIM	**C**entralized **T**elephone **I**nterconnect **M**odule − The CTIM is a CEC/IMC interface module used to connect **C**entralized **T**elephone **I**nterconnect **S**ystem (**CTIS**) equipment to the switch so radio users and dispatchers can access land-line telephone systems.
DATA	(see **EDG interface module**)
daemon	Background process that performs system-wide functions.
distributed multisite	Two or more IMC networks can be linked together for **distributed multisite** communication. Audio, mobile data/Aegis data and control data is transferred between the different IMC networks via a NIM at each IMC switch. (Also see **StarGate Controller**.)
DPRAM	**D**ual **P**ort **R**andom **A**ccess **M**emory − These specialized memory chips have two separate data buses that allow two microprocessor chips to quickly and efficiently transfer data between each other.
DVIM	**D**igital **V**oice **I**nterface **M**odule − The DVIM is a CEC/IMC interface module that connects **D**igital **V**oice **I**nterface **U**nits (**DVIU**) to the switch to provide Aegis digital and Aegis private voice operation for dispatch consoles and CTIS equipment.
DVIU	**D**igital **V**oice **I**nterface **U**nit. Provides digital interface to the dispatch console and enables digital mode communications with the console operator.

TERM	DEFINITION
EDACS	EDACS, short for **E**nhanced **D**igital **A**ccess **C**ommunications **S**ystem, is a registered trademark of Ericsson Inc. It is used by Ericsson to describe specific communications systems and their specific equipment which meet or exceed the needs of the Public Service, Industrial, Commercial, and Utility markets world-wide.
EDACS radio system	**E**nhanced **D**igital **A**ccess **C**ommunication **S**ystem **radio system** − The term "EDACS radio system" refers to RF equipment that may be interfaced to the EDACS CEC/IMC switch. The RF equipment may be located at a single location, such as an EDACS site or it may be located at several locations, such as in a voting system. Other examples of EDACS radio systems include simulcast, CNI, and SCAT systems.
EDG	**E**DACS **D**ata **G**ateway. Provides landline group and individual data calls for EDACS networks.
EDG interface module	**E**DACS **D**ata **G**ateway **interface module** − Mobile data is forwarded to the CEC/IMC switch from the EDG computer equipment via the **EDG interface module**.
ELI	Enhanced Local Interconnect. In EDACS trunking, a telephone switching system that allows authorized radio users to make and receive telephone calls without dispatcher assistance.
FCAPS	Standard term that stands for the five broad areas of network management: **F**aults, **C**onfiguration, **A**ccounting, **P**erformance, and **S**ecurity.
GETC	Ericsson **G**eneral **E**lectric **T**runking **C**ard − The GETC is a microprocessor-controlled shelf that can be configured to perform many different signal processing tasks for Ericsson GE radio communications equipment. In CEC/IMC applications, each GETC is equipped with a 9600 baud modem that provides serial control data communications between the CEC/IMC (Uplink GETC) and different radio systems (Downlink GETC).
Graphical User Interface	A **G**raphical **U**ser **I**nterface (GUI) is a way of communicating with a computer by manipulating icons (pictures) and windows with a mouse.
GSC bus	**G**lobal **S**erial **C**hannel **bus** − The GSC bus is a high-speed serial bus that provides packetized control data transfers between Controller Boards in the CEC/IMC switch.
GUI	See Graphical User Interface.
HDI	EDG **H**ost **D**ata **I**nterface. Provides an interface to host computers using RDI protocol.
HDLC	High-Level Data Link Control protocol. A link level protocol standard by ISO that is the basis for several link layer protocols.
HP OpenView	A suite of system and network management products offered by Hewlett-Packard.

TERM	DEFINITION
HP OV NNM	Hewlett-Packard **O**pen**V**iew **N**etwork **N**ode **M**anager. Management platform that provides common management functions, such as data collection and reporting, using standard protocols and software interfaces.
Hub	Used to concentrate several 10BaseT (Twisted Pair Ethernet) onto coaxial Ethernet. OSI physical layer only.
IEA	Integrated EDACS Alarm.
IMC	**I**ntegrated **M**ultisite and **C**onsole **C**ontroller − The Ericsson GE IMC is a digital audio switch that routes audio/mobile data/Aegis data between EDACS radio systems and dispatch consoles. It is a second generation multisite controller plus a console controller for the C3 series consoles.
IMC Node Icon	The IMC Node icon consists of a Switching Center.
Internet	A set of networks connected by IP routers and appearing to its users as a single network.
Internet Protocol	The Internet Protocol (IP) is the TCP/IP layer 3 protocol responsible foe transporting datagrams across the network.
IP Address	An IP (Internet Protocol) address is the numeric identifier address of an element.
ISDN	Integrated Services Digital Network. A set of CCITT standards aimed at integrating voice and data services. ISDN provides end-to-end digital services. Allows for interconnection of remote systems and LANs over an ISDN network for applications running on top of the standard TCP-IP protocol.
Jessica	Ericsson's tradename for a Private Branch Exchange (PBX) Gateway for telephone interconnect via a central network node.
LAN	Local Area Network. A short-distance data communication system that uses moderate to high data rates (100 kb/s to 50 Mb/s). The network interconnects a group of computers to provide intercommunication, sharing of data files, software, and printers.
LAPB	A modified form of HDLC that CCITT chose as the link level protocol for X.25 networks. LAPB provides for the reliable transfer of a packet from a host to an X.25 packet switch, which then forwards the packet to its destination.
LRIM	**L**ogging **R**ecorder **I**nterface **M**odule − This CEC/IMC interface module provides audio outputs for logging recorders. Each output channel can be programmed to supply audio based on groups or individual units within the CEC/IMC network.
Managed Object	An object holding network management information, characterized by an identifier, a value, implementation requirements, and valid operations.

<u>TERM</u>	<u>DEFINITION</u>
Management Information Base	Management Information Base. A description of the data stored in a Network Element similar to a C structure. A MIB definition allows the EDACS Network Manager to read and write values in a Network Element.
MAU	Multistation Access Unit. A transceiver for LAN connections.
ME	Management Element. An EDACS platform that configures EDACS NEs. Examples of MEs are CEC/IMC Manager, EDACS 4 Radio Programmer, EDACS Network Manager, System Manager, PI terminal, EDG terminal, etc.
Media Access Control (MAC)	A protocol governing a station's access to a network.
MIB	See Management Information Base.
MIM	**M**ASTR II/III **I**nterface **M**odule − The MIM connects an EDACS radio system to the CEC/IMC switch. EDACS radio systems include EDACS sites, simulcast systems, voted systems, CNI and SCAT systems.
MOM	**MO**nitor **M**odule − The MOM is a CEC/IMC interface module that provides serial data connections for the CEC/IMC Manager (MOM PC) and the System Manager computers.
MOM PC	(see **CEC/IMC Manager**)
Multiple Access Unit (MAU)	For a Token Ring, a concentrator used to connect multiple stations to the ring.
multisite	A **multisite** is a network of multiple EDACS radio systems and possibly conventional radio systems all linked together for wide-area communication. In a multisite network, adjacent systems do not use the same radio frequencies. Each system networked may have a different number of working channels.
Native Proxy	Proxy that communicates with its agents via SNMP.
NE	**N**etwork **E**lement. An EDACS platform that provides links in the EDACS network for either digital voice, analog voice, data, or control information. IT IS NOT A PLATFORM USED TO CONFIGURE EDACS NEs. Examples of NEs are IMC, GETC, Site Controllers, PIs, etc.
Network Address	The 32-bit IP address of a system.
Network Manager	The EDACS Network Manager is a UNIX workstation or server that provides EDACS administrators with a consistent, integrated view of the alarm status of their EDACS network.
Network Number	A network is a logical association of IMC, StarGate, CEC, and Remote CEC nodes. The Network Number identifies the nodes for which the traffic will be monitored by the Multisite Monitor.
NIM	**N**etwork **I**nterface **M**odule − Two or more IMC networks can be linked together for distributed multisite communications using a NIM at each IMC switch.

<u>**TERM**</u>   <u>**DEFINITION**</u>

TERM	DEFINITION
NM	See Network Manager.
Node	A terminal of any branch of a network, or a terminal common to two or more branches.
Node Number	This is the EDACS Node Number which uniquely specifies an IMC/CEC/StarGate in the EDACS network.
Object Identifier	A string of numbers derived from a global naming tree, used to identify an object.
OpenView	See HP OpenView
PCM	**P**ulse **C**ode **M**odulation − An audio processing technique used to encode and decode analog signals so they can be transferred digitally.
PDU	**P**rotocol **D**ata **U**nit. Grouping of data defined within SNMP.
PI	**P**rivate Branch Exchange **I**nterface. The Jessica VMEbus chassis provides connectivity between the IMC and the MD110.
PMU	**P**ower **M**onitor **U**nit. This EDACS unit monitors the output power of the transmitters and the VSWR of the antenna system. If a fault occurs, it sends an alarm to the Site Controller. The PMU is co-located with the Site Controller computer.
Port	A point for accessing a device, circuit, or network. For a bridge, an interface to a LAN or point-to-point link.
Privacy	Protection of the contents of a message by means of encryption.
Proxy Agent	An agent that responds to requests from one or more managers by polling remote devices. A proxy also relays traps generated by devices under its supervision to other managers.
PSTN	**P**ublic **S**witched **T**elephone **N**etwork. The communication system that links telephones nationwide by means of loops, trunks, and switches owned and operated by the public telephone companies. The term is often used for data and other non-telephone services carried over the telephone network.
Radio Switch	Term used to designate the CEC, IMC, or StarGate.
RCEC	Remote Console Electronics Controller.
RCEC Node Icon	The RCEC Node icon consists of the RCEC and Consoles.
Request For Comments (RFC)	The RFC is a set of documents containing Internet protocols and discussions of related topics. These documents are available on-line at the Network Information Center.
RIM	**R**equest Status Monitor **I**nterface **M**odule − The RIM interface module

TERM	DEFINITION
	enables the RSM computer to request status information from radios within the network.
Router	A system used to connect separate LANs and WANs into an internet, and to route traffic between the networks. In the Network Manager system, a router is needed to go from Ethernet to T1 physical media. OSI Network, Data Link, and Physical Layers only.
RS-232	A type of serial interface typically used for terminals, modems, and printers.
RSM	**R**equest **S**tatus **M**onitor − The RSM is an IBM PC compatible computer running custom software developed by Ericsson GE. It allows the system administrator and/or the dispatchers to view status of EDACS units within the CEC/IMC network. Status information is typically initiated (transmitted) by the radio operator to identify the current condition (in route, at scene, etc.) of the unit.
SCAT	**S**ingle-**C**hannel **A**utonomous **T**runking. In EDACS, SCAT is a trunked system consisting of a single failsoft repeater and a downlink GETC. Operationally, it functions as a control channel or a working channel, depending on the trunked service required. In its idle state, SCAT operates as a control channel. When a channel request is made, SCAT assigns the call to itself and converts to a working channel. EDACS address hierarchy is maintained as are many trunking features.
Shell	An HP-UX command interpreter (CSHELL, KORN, etc.), providing a working environment interface for the user. When user logs in, the Session Manager starts HP VUE applications that were running during a previous session.
Simple Network Management Protocol	The Simple Network Management Protocol (SNMP) is a protocol that enables a management station to configure, monitor, and receive trap (alarm) messages from a Network Element. It also provides additional administrative structure, authentication, and privacy.
Simulcast	Simultaneous Broadcast by two or more transmitters located at different sites operating on the same RF frequency.
site	This term normally refers to EDACS radio equipment at a single specific location.
Site Controller	A computer running Ericsson-developed application software that controls the moment-to-moment trunking process, plus such features as call validation, unit enable/disable, dynamic regrouping, and queuing management. The Site Controller communicates with the System Manager over an appropriate link.
Site Icon	The Site icon consists of physical devices located in one geographic location such as the Site Controller, ELI, ACU, PMU, TU, and Channels.
Site Number	This is the EDACS Site Number which uniquely identifies the Site on a particular Node.
SM	See System Manager.

<u>**TERM**</u>	<u>**DEFINITION**</u>
SNMP	See Simple Network Management Protocol.
StarGate	In EDACS trunking, links up to eight EDACS wide-area multisite networks to create a single, seamless network.
StarGate Controller	A **StarGate Controller** is an IMC switch specifically configured for distributed multisite operation. It is the central point or "hub" for all distributed multisite communications.
SubSite Number	This is the EDACS SubSite Number which uniquely identifies the SubSite device on a particular Node. A channel is a subsite device.
super user	The root user who has special privileges. Same as the System Administrator.
Switching Center	Collection of node level devices physically connected to the IMC. These devices include the PI, BCU, CAL, EDG, and Consoles.
System Manager	The **System Manager** is a DEC multitasking computer which performs features such as monitoring system operation, generating management reports, individual unit enable/disable and dynamic regrouping.
T1/E1	Digital landline and microwave transmission standards used in the United States and Europe.
TCP	**T**ransmission **C**ontrol **P**rotocol. A connection-oriented protocol with acknowledgments and retries.
TDM	**T**ime **D**omain **M**ultiplexing. Technique used to multiplex multiple signals onto a single hardware transmission channel (bus) by allowing each signal to use the channel for a short time before going on to the next one.
TDM bus	**T**ime **D**ivision **M**ultiplexed **bus** − The TDM bus in the CEC/IMC switch is a digitally multiplexed bus system used to transfer audio/mobile data/Aegis data throughout the CEC/IMC switch. Each signal coming into the CEC/IMC switch is assigned a TDM time slot and receiving devices extract the digitized signals from the appropriate time slot.
Technician (or Tech or EDACS technician)	Customer personnel whose main responsibility is to install, maintain, and troubleshoot individual EDACS platforms, such as GETCs, Site Controllers, EDGs, and IMCs. Technicians require software interfaces that run on common laptop/desktop personal computers to assist in hands-on setup of a particular platform.
Telnet	The TCP/IP protocol that enables a terminal attached to one host to log into other hosts and interact with their applications. It is the Standard internet protocol for terminal emulation.
TFTP	Trivial File Transfer Protocol. A basic TCP/IP protocol used to upload or download files. Typically uses include initializing diskless workstations.
tracking	In a multisite network, all active radios log into their particular system. This

TERM	DEFINITION
	login information is databased to allow the CEC/IMC to track individual radio units as they move from system-to-system. The CEC/IMC can then route wide area calls based on this database.
Transmission Control Protocol	The Transmission Control Protocol (TCP) is the TCP/IP protocol that provides reliable, connection-oriented data transmission between a pair of applications.
Trap	A message that reports a problem or significant event.
Trunking	The process of dynamically allocating a limited number of radio channels to groups of people for communication purposes.
TSI	EDG **T**runked **S**ystem **I**nterface. The TSI handles all communications to the rest of the EDACS trunked radio system via the CEC/IMC CIM.
TU	Test Unit. The TU continually tests channels and provides an alarm to the Site Controller if a fault is detected. The TU and ACU form the Test and Alarm Unit (TAU).
UDP	User Datagram Protocol. Connection-less-mode transport protocol used by SNMP. Does not use acknowledgments or retries.
UPS	Uninterruptible Power Source. Used to keep the system running in the event of a power outage.
VMIM	Con**V**entional **I**nterface **M**odule − The VMIM couples the CIA secondary interface rack to the primary CEC/IMC switch interface modules. The VMIM - CIA set allows conventional base stations and conventional satellite receiver voting systems to be connected to the CEC/IMC switch.
X-model	A network-based display device that uses the X protocol over LAN to communicate with the host.
X-terminal	The high-end performing X-model targeted at technical environments.
XLTR	C3 Modular/Desktop Console **Translator** − Using data protocol conversion techniques, this interface module allows the CEC/IMC switch to communicate with a C3 Modular/Desktop console. The XLTR is placed in the control data path between the C3 console and its respective CIM.

17. INDEX