LBI-39215

System Manual

EDACS® NETWORK MANAGEMENT

ERICSSON

NOTICE!

This manual covers Ericsson and General Electric products manufactured and sold by **Ericsson Inc**.

NOTICE!

This product may only be used for the functions described in this manual. Use of the product for other purposes shall constitute a violation of the license. Moreover, any addition of non-Ericsson approved hardware and software may cause the product to malfunction.

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. PREFACE

This is one of four manuals for the EDACS® Network Manager. This manual provides a system level overview and provides background information about the Network Management program, its specification, capabilities and features. It also serves as a guide for persons planning and developing the Ethernet Network.

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

- *EDACS Network Manager User's Guide* (LBI-39169):
  This manual contains information for using the Network Manager system.
- *EDACS Network Manager Enterprise Management Information Base (MIB) Technical 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. It also includes troubleshooting information.

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	**Network Manager Specifications** - The Specifications section identifies the hardware and software specifications and compatibility with other platform hardware and software.
Section 3	**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 4	**EDACS Network Management Overview** - Presents the Network Management and Network Manager architecture and summarizes the features of the EDACS Network Manager. The section also presents the hierarchy of map levels and icons used to logically categorize the EDACS devices.
Section 5	**EDACS NM Menus and Their Functionality** - This section describes the actions performed on the EDACS devices (icons) through the use of pulldown menus.
Section 6	**EDACS Map Generation and Propagation** - This section provides an overview of the Network Manager's process for generating hierarchical maps.
Section 7	**OpenView Network Node Manager Features** - The EDACS Network Manager leverages HP OpenView Network Node Manager as much as possible. This section lists some of the features provided by OpenView.
Section 8	**Network Planning** - This section provides information for use by system engineers and designers which will aid in identifying system requirements and designing the Network Manager system.
Section 9	**FCAPS** - This section details the five functional areas of, **C**onfiguration, **A**ccounting **P**erformance, and **S**ecurity (FCAPS) identified by the Network Management forum of the International Organization for Standards.
Section 10	**Glossary** - Contains a glossary of terms.
Section 11	**Network Manager Survey** - This survey identifies the customer's specific system requirements. The information will allow system engineers to initially configure the Network Manager station.

2. EDACS NETWORK MANAGER SPECIFICATIONS

2.1 REGULATORY STATEMENTS

The EDACS Network Manager has FCC Part 15, Class B approval, CSA approval, and UL approval, and carries the CE Mark of approval for the European union.

Safety and regulatory statements for the Network Manager equipment may be found in the accompanying Owner's Guides supplied with each computer system.

2.2 PHYSICAL SPECIFICATIONS

The Network Manager is available in three models: NM0, NM1, and NM2. Their use depends on the system size as determined by the number of managed network elements and the number of simultaneous users. Each model will contain the following:

	NETWORK MANAGER CONFIGURATIONS		
	NM0	**NM1**	**NM2**
GENERAL SPECIFICATIONS:			
HP 9000 - 700 Series Workstation	712/60	N/A	N/A
HP 9000 - 800 Series Server	N/A	G60	G60
PA-RISC Processor	60 MHz	100 MHz	100 MHz
Internal RAM Mbytes (base)	64	128	512
Maximum Users/EDACS Network Elements	1/1000	3/2000	5/15000
	2/100	5/500	25/500
17-inch color monitor or 17-inch Envisex X-Terminal	yes	yes	yes
4 gb DDS Tape Drive	yes	yes	yes
CD-ROM Drive	yes	yes	yes
Disk Drive	One - 2 gb	Two - 2 gb	Two - 2 gb
HP OpenView Network Node Manager Software	yes	yes	yes
IMC Support	yes	yes	yes
VAX System Manager Support	yes	yes	yes
JESSICA/BCU/CAL	yes	yes	yes
Remote Access	yes	yes	yes

	NETWORK MANAGER CONFIGURATIONS		
	NM0	**NM1**	**NM2**
EXPANDED CONFIGURATION:			
Maximum RAM Mbytes	128	768	768
Upgrade to 712/100	yes	N/A	N/A
Upgrade to G70 (Dual Processor)	N/A	yes	yes
POWER REQUIREMENTS:			
Operating Voltage: (Auto Selecting)	110-120 Vac, 2.7A (max) 220-240 Vac, 1.2A(max)	110-120 Vac, 6.0A (max) 220-240 Vac, 3.0A (max)	
Nominal Frequency:	50 - 60 Hz	50 - 60 Hz	
Power Requirements:	110 Watts (max)	800 Watts (max)	
PHYSICAL CHARACTERISTICS:			
Dimensions (Height x Width x Depth): (excludes keyboard or monitor)	12 cm x 42 cm x 39 cm (4.9 in. x 16.5 in. x 15.3 in.)	43 cm x 44 cm x 53 cm (17 in. x 17.5 in.x 21 in.)	
Weight:	9 kg (20 pounds)	50 kg (110 pounds)	
Heat Dissipation:		2770 Btu/h	
ENVIRONMENTAL CHARACTERISTICS:			
Temperature Range (ambient air temperature)			
Operating: Storage	5° to 40°C (41° to 104°F) -34° to 50°C (-30° to 122°F)		
Relative Humidity			
Operating: Storage:	20% to 80%, non-condensing 5% to 80%, non-condensing		

The NM0 configuration can be enhanced by adding 64 Mb of RAM, and further performance improvement can be achieved by upgrading the 712/60 processor to the 712/100 processor. Expanding the NM0 configuration will permit support for additional managed Network Elements (approximately 2500). The 712/100 can support a maximum of 196 Mb of RAM.

The NM1 and NM2 configurations can be enhanced by adding RAM in 128 Mb segments to a maximum RAM size of 786 Mb and by adding additional disk drives. Additional users also require an 8-user or higher license. An upgrade to the Model G70 Business Server may be required to support the performance desirable with 25 simultaneous users.

The G60 has two 2 Gb hard drives. HP offers a software option to make these mirrored disks.

2.3 NETWORK MANAGER SIZING ALGORITHM

The type and size of the Network Manager configuration (NM0, NM1, or NM2) is determined by two (2) factors:

1. The number of managed elements (icons) and,
2. The number of concurrent OpenView users.

The following algorithm is used to determine the amount of memory required by UNIX and OpenView which uses the majority of RAM. There are other processes which use memory that are not accounted for here. Approximately 22% above the OpenView size should be reserved for these processes.

A managed element is any OpenView element represented by an Icon. The following items will constitute a managed element:

IMC	CEC	Remote CEC
Site	StarGate	Jessica PI
BCU	CAL	EDG
System Mgr. (VAX Only)	Maestro Console	Site Controller
ACU	PMU	Test Unit
Channel (GETC)		

An OpenView user is any user to be executing the Network Manager application from an X-Station or from an X-Session on a PC.

The following variables will be used in the NM sizing algorithm:

m Managed element = **1 ea. of the above listed items**
p Number of simultaneous users

$$\mathbf{RAM = (15M + 20k \times m + p \times 20M) \times 1.22}$$

NOTE: The algorithm accounts for a maximum of 5 Mb for Background Graphics.

When specifying a Network Manager station to a customer, the number of planned users and planned Network elements will determine the amount of additional RAM to be added.

The table below lists the Network Manager options:

Table 1 - Network Manager Station RAM Availability

Network Manager Station Configuration	RAM (megabytes)
NM0	64
NM0 + additional memory option	128
NM1	128
NM1 + additional memory option	256
NM2	512
NM2 + additional memory option	768

2.4 SOFTWARE COMPATIBILITY

The Network Manager Application is functional when the following Software Packages/Versions have been loaded on a suitable HP workstation or server.

Table 2 - Network Manager Software Requirements

Product	Version
OpenView Network Node Manager	3.31
HP-UX	09.05
TSSterm 420 for HP9000	2.0.2
Network Manager Platform Software	350A1900

The Network Manager 350A1900 platform software is designed to be compatible with the following EDACS versions:

Table 3 - EDACS Platform Software Compatibility

PLATFORM	MINIMUM VERSION*	RECOMMENDED VERSION
IMC Software Controller Boards : - 344A3567G12 (U58) - 186 MP - 344A3568G12 (U59) - 186 MP Ctrl. Board Interface : - 344A3565G12(U3) - 152 MP	3.04	5.03
CEC/IMC Manager (for NT) 344A3630G12	5.03	5.03
CEC/IMC Manager SNMP Agent AE/LZY 213 765 R1E	1.05	1.05
System Manager Software Core Config - TK50 (344A4067G6) - DAT (350A1816G6) Mid Config - TK50 (344A4582G6) - DAT (350A1817G6) Full Config - TK50 (344A4583G6) - DAT (350A1818G6)	6.02	6.02
System Manager NM Interface (Multinet) w/ a patch tape TK50 - 350A2026G6 DAT - 350A2030G6	3.50	3.50
Networks/Data VME Controller ROM 349A9983G4	3.05	3.05
BCU/CAL 350A1103G3	1.02	2.03
PI 349A9982G4	3.01	3.01
CEC/IMC Manager HP-UX Client 350A2001G1	5.09	5.09
Site Controller	7.07	7.07

CXC 112 1272 R8A		
GETC GETC STATION : GETC (349A9607G6) TURBO (344A4414G6) GETC LINK : GETC (344A4895G6) TURBO (350A1121G6)	All	6.00

* NOTE: The minimum software version may have some functionality deficiency. Refer to section 2.5, BACKWARDS COMPATIBILITY:

2.5 BACKWARDS COMPATIBILITY

2.5.1 CEC/IMC Manager

CEC/IMC Manager for NT is required to receive any IMC faults or performance. Earlier versions will not adversely affect the Network Manager program nor will they support the Network Manager program. THe CEC/IMC Manager for NT is required to support the CEC/IMC Manager HP-UX Client.

2.5.2 IMC

The CEC/IMC Manager for NT requires the IMC recommended version. Earlier IMC versions will partially support Network Manager performance as indicated in the Performance section.

2.5.3 Site Controller/GETC

The Site Controller recommended version and the GETC recommended version support four new alarms: GETC Voter Failure, GETC Turbo Failure, GETC Power Failure, and GETC Synthesizer. All earlier versions will forward their existing faults to the Network Manager.

2.5.4 System Manager

System Manager versions prior to the recommended version will neither support nor hinder the Network Manager feature. System Manager platforms must also have the SNMP Agent (TGV's Multinet) installed.

NOTE: Versions of the TGV Multinet SNMP Agent other than the recommended version are untested and may prove incompatible with the current version of Network Manager.

2.5.5 PI

The PI recommended version is required for PI faults and PI specific performance. See the performance section.

2.5.6 BCU/CAL

The BCU/CAL recommended version is required to get BCU/CAL faults. See the performance section.

Performance:

Two Dimensional Line graphs are only available with the recommended versions of the PI and BCU indicated above. MultiSite Monitor and Site Monitor are available with BCU/CAL minimum version. The MultiSite Monitor and Site Monitor will function with IMC Software versions as early as minimum version with minor performance degradation.

The following features are not available with IMC Software earlier than Group 11.

- The User Interface "**`stat`**" command on BCU/CAL and "**`traf`**" command on PI will not provide information regarding Queued, Denied, System Busy, and Convert-To-Callee channel events.
- MultiSite and Site Monitoring and Two Dimensional Line graphs will not reflect Queued, Denied, System Busy, and Convert-To-Callee channel events.
- The MultiSite and Site Monitor will not provide control channel indication for sites.

3. DOCUMENTATION

In may be necessary to consult one or more of the following documents when installing or maintaining the Network Management system. These manuals will also provide additional guidance if you encounter technical difficulties during the installation or configuration process.

3.1 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

3.2 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.

4. EDACS NETWORK MANAGEMENT OVERVIEW

The Enhanced Digital Access Communications System (EDACS) has rapidly grown from a simple trunked radio system to a complex, multi-faceted heterogeneous communications network. This network, consisting of not only EDACS equipment, but also microwave, Computer-Aided Design (CAD), networking, and other equipment has necessitated a centralized network management approach. Ericsson has responded to this need with EDACS Network Management.

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. Ericsson's strategy for consolidated user interfaces replaces some local user interfaces with client/server interfaces which can be run locally or remotely at the EDACS Network Manager (NM) station, as well as allowing native access via Telnet session. The client/server relationship is implemented using Open Systems Foundation (OSF) standard Remote Procedure Calls (RPCs) to accomplish communication. For example, on the EDACS NM the administrator can view a graphical map of an EDACS network in one window, run a Console Electronics Controller (CEC) and Integrated Multisite and Console Controller (IMC) Manager session in another window, and Telnet into the System Manager in a third window.

The EDACS Network Manager provides a hierarchical representation of the EDACS network based upon the industry standard Simple Network Management Protocol (SNMP) and is a Hewlett-Packard (HP) OpenView (OV) Network Node Manager (NNM) application. OpenView NNM allows multi-vendor components, including hubs, bridges, routers, and various computers, to be managed on the same maps as EDACS elements. Leveraging OpenView NNM provides easy integration with third-party applications to handle needs such as trouble ticketing and paging.

There are five fundamental areas of network management: Faults, Configuration, Accounting, Performance, and Security (FCAPS). Network Management focuses on Faults and Performance while starting the transition for centralizing the Configuration of EDACS. As several EDACS platforms are networked together with Transmission Control Protocol/Internet Protocol (TCP/IP), billing and report information can be easily transferred to the EDACS Network Manager for printing, or may be printed directly to a network printer.

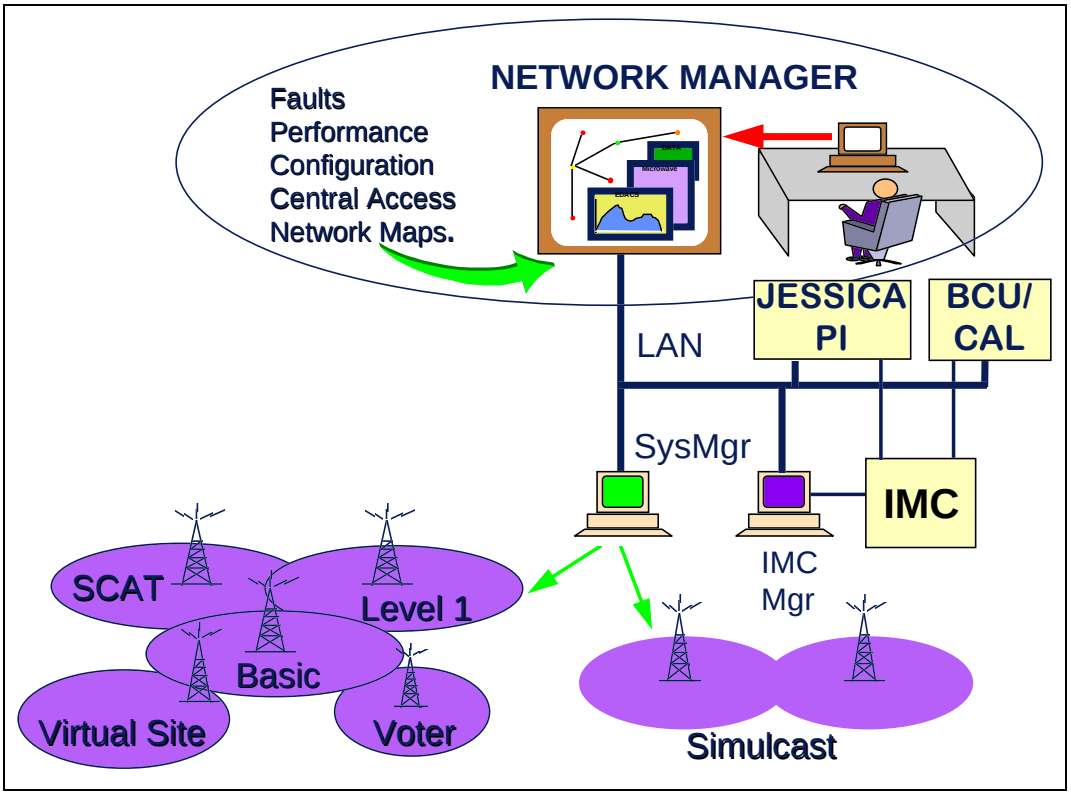


Figure 1 - Network Management Single Point Of Control

4.1 SOFTWARE FEATURES

The following table provides a convenient list of features found in the current version of the Network Manager software.

Table 4 - EDACS Network Manager Features

FEATURE	DESCRIPTION
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.
Fault Notification	EDACS platforms send all alarm and status event information to one point. Events are logged at the EDACS Network Manager and pictorially displayed on the hierarchical graphics.
Hierarchical Network Map for Fault Notification	EDACS administrators have one Network Management Station that provides a consistent, integrated view of the alarm status of their EDACS network. Alarms are propagated from lower network layers all the way up to the entire network view.
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.
Graphical Performance Monitoring	EDACS 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.

FEATURE	DESCRIPTION
Site Monitor	The Site Monitor oversees call activity for an individual site. It is available with BCU/CAL or as a separate PI option.
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.
Telnet Sessions to PI, EDG, BCU, CAL, and System Manager	The ability to log in to multiple platforms and operate in their native modes from one terminal provides a nice migration path for current EDACS users. Access to these sessions is built into the network user interface menus.
Basic Help Menu	On-line help for the EDACS Network Manager application is available.
Alarm Help	On-line help describing the fault and, where possible, suggesting action to take to remedy alarms is accessible. In addition to the EDACS-provided alarm information, the customer may add his own text for site-specific alarm help/corrective action suggestions.
Remote Operation/Logging User Actions	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.
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.

4.2 NETWORK MANAGEMENT ARCHITECTURE

Figure 2 shows the EDACS network from a management perspective. Not all EDACS elements are accessed directly by the EDACS Network Manager. In some cases, an EDACS device acts as a proxy for other EDACS devices. In Figure 2, the System Manager connected to the TCP/IP LAN has an SNMP agent which will proxy for devices shown connected to it, such as the SIM or Site Controller.

The LAN Network consists of the EDACS Network Manager (NM), CEC/IMC Manager for NT, EDACS Data Gateway (EDG), PI, BCU/CAL, and System Manager. The System Manager proxies alarm information for the ACU, PMU, TU, SC, and GETC. The CEC/IMC Manager proxies alarm information for the CEC/IMC and all links connected to it. The EDACS NM provides full management services to the CEC/IMC Manager, PI, BCU/CAL, and System Manager Network Elements (NEs). The EDACS NM is also involved during the troubleshooting of these elements.

The detailed block diagram in Figure 3 shows one node of an EDACS network. This figure demonstrates the advantages of centralized network management with the numerous possible links and devices composing even one node in a network. One possible means of connecting two IMCs is shown in Figure 4. A T1 interface is used to connect the two routers leading to the IMCs.

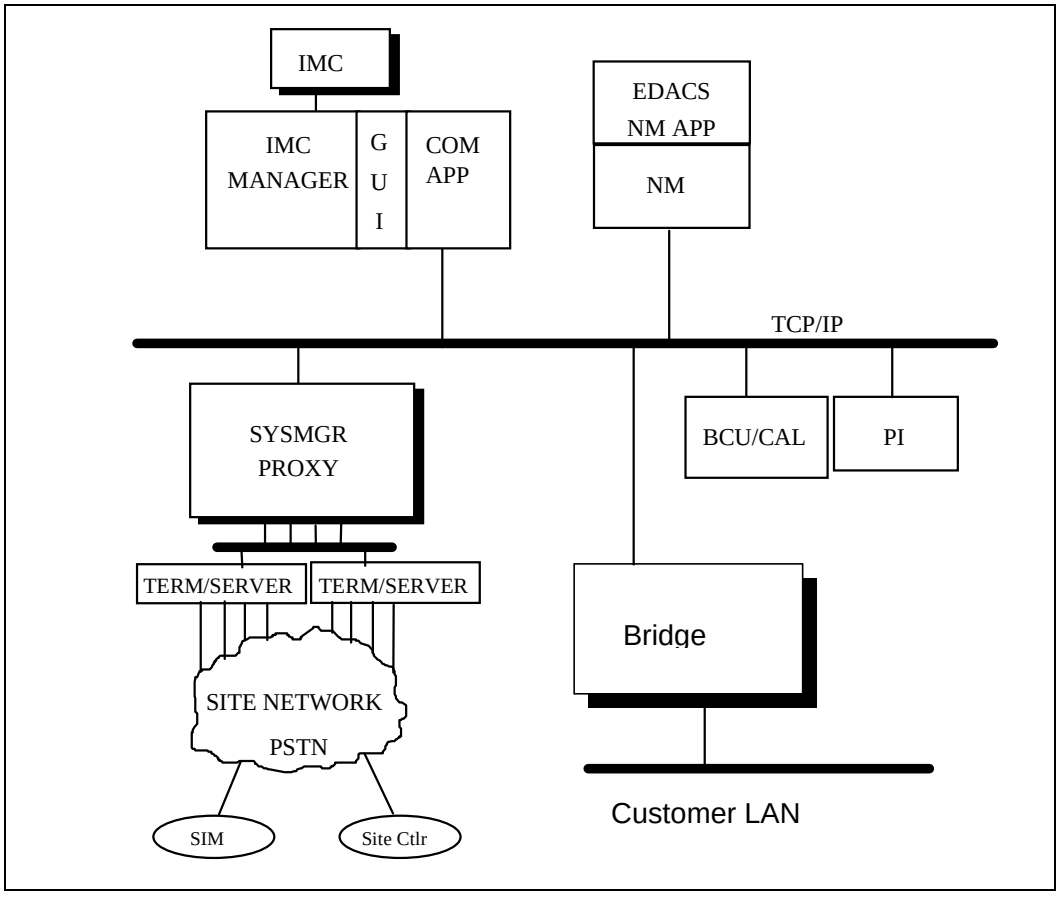


Figure 2 - High-level Network Block Diagram

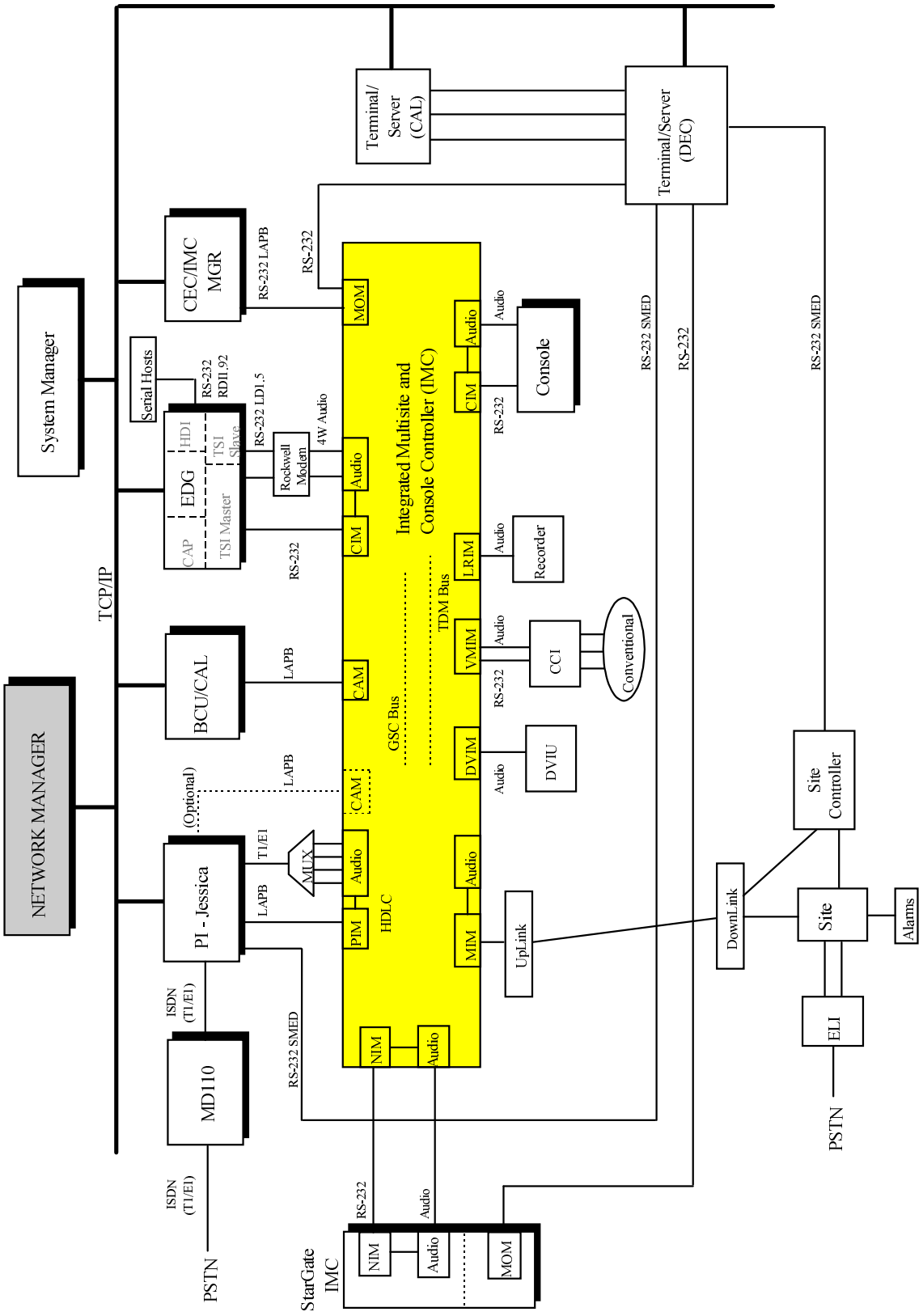


Figure 3 - EDACS Detailed Network Block Diagram

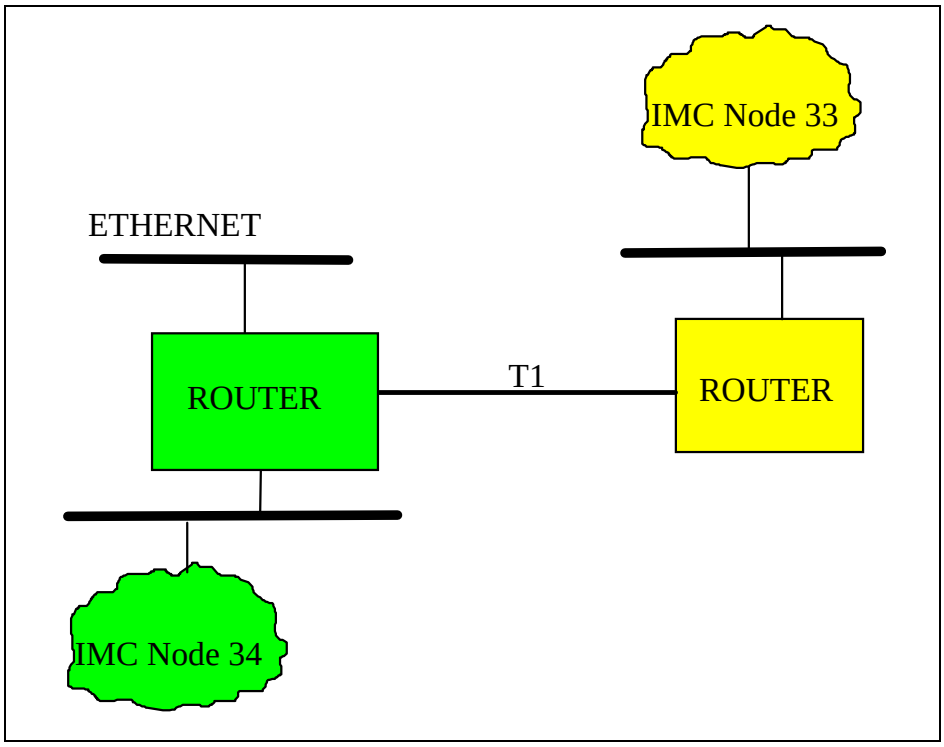


Figure 4 - Internodal Connectivity

4.3 NETWORK MANAGER ARCHITECTURE

The Network Manager Architecture is consists of three basic elements; Standard Management Protocols, an Open Management Platform, and a large library of Management Applications as shown in Figure 5:

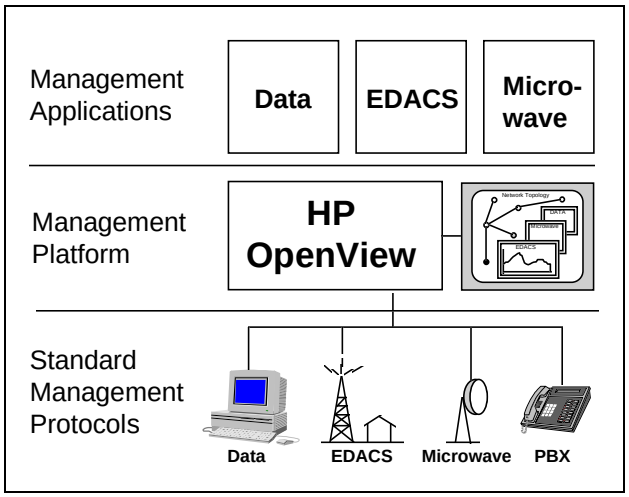


Figure 5 - Network Management Layers

4.3.1 Standard Management Protocol

The foundation of the Network Management System is the standard management protocol that exchanges data with all network devices in the same way. The Network Management System uses the Simple Network Management Protocol (SNMP) as the Standard Management Protocol.

SNMP is a widely supported protocol and is considered the industry standard. It allows the Network Manager to read and write management data stored in the Management Information Base (MIB) of each device. The protocol also enables the network devices to notify the Network Manager of status changes or alarm conditions.

NOTE: The management platform can also support a CMIP protocol option.

4.3.2 Management Platform

The Network Management platform consists of a UNIX workstation or server running EDACS applications integrated with Hewlett-Packard (HP) OpenView (OV) Network Node Manager (NNM) software that provides the EDACS administrators with a consistent, integrated view of the alarm status of their EDACS networks. The platform serves as a host to local sessions and participates as a server for the main EDACS topology database. It also handles many of the low level management functions and provides a framework to ensure all 3rd party applications have the same look and feel. The platform also combines information from all network elements, regardless of the vendor, in a homogeneous way which enables the user to see the big picture and quickly identify problems.

A simplified view of the management platform is shown in Figure 6. The platform contains four major elements: communication, common management functions, user interface and applications interface.

The Communications section coordinates the data exchange with network elements using SNMP.

The Common Management Functions block can be subdivided into network monitoring, alarm processing and performance monitoring. Network monitoring involves “polling” each address on the network (i.e. sending a message and waiting for the response). This allows OpenView to detect new IP elements on the network and to verify that known IP elements are still on line. The alarm processing function stores network alarms in a database for tracking and reporting, updates the display, and triggers user defined actions such as sounding an audible alarm or issuing a page to the appropriate person. Performance monitoring involves collecting MIB values from any combination of network elements and continuously graphing the results to summarize network performance. This function is extremely useful for detecting bottlenecks and degradation of service.

The User Interface ties all of the management information together through a graphical network map and integrated menu system. The Network Manager uses HP OpenView Network Node Manager as its management platform. OpenView NNM using an advanced graphical user interface is a familiar environment to most PC users and extremely flexible. For example, on this platform the administrator may view a graphical map of an EDACS network in one window, run a CEC/IMC Manager session on another, and log in to the System Manager for configuration on a third site. The platform also allows you to use third party applications such as trouble-ticketing or paging to customize and enhance the functionality of the Network Manager.

The Application Interface provides standard interfaces to the platform functions allowing management applications to build on the foundation established by the platform. The application interface also ensures that applications from different vendors work in concert to produce the appearance of a single product with a consistent interface and operation.

4.3.3 EDACS Management Application

The final element of the Network Manager contains Management Applications which flesh out the skeleton provided by OpenView. These applications include product specific management programs and integrated management support tools. Though many management functions could be handled by OpenView alone, an extensive amount of time would be required to configure the platform for each network element. Product specific applications, provided by many network vendors, eliminate the need for most user configuration by supplying icons, proper polling and alarm defaults, pre-configured performance graphs and reports. The Network Manager includes an EDACS application specifically designed to manage EDACS equipment.

The complete Network Management strategy includes SNMP support on the EDACS devices, and HP OpenView on a UNIX workstation or Server, with the EDACS Network Manager Application. You can then add other OpenView based product specific applications, or management support tools to customize the Network Manager to your network.

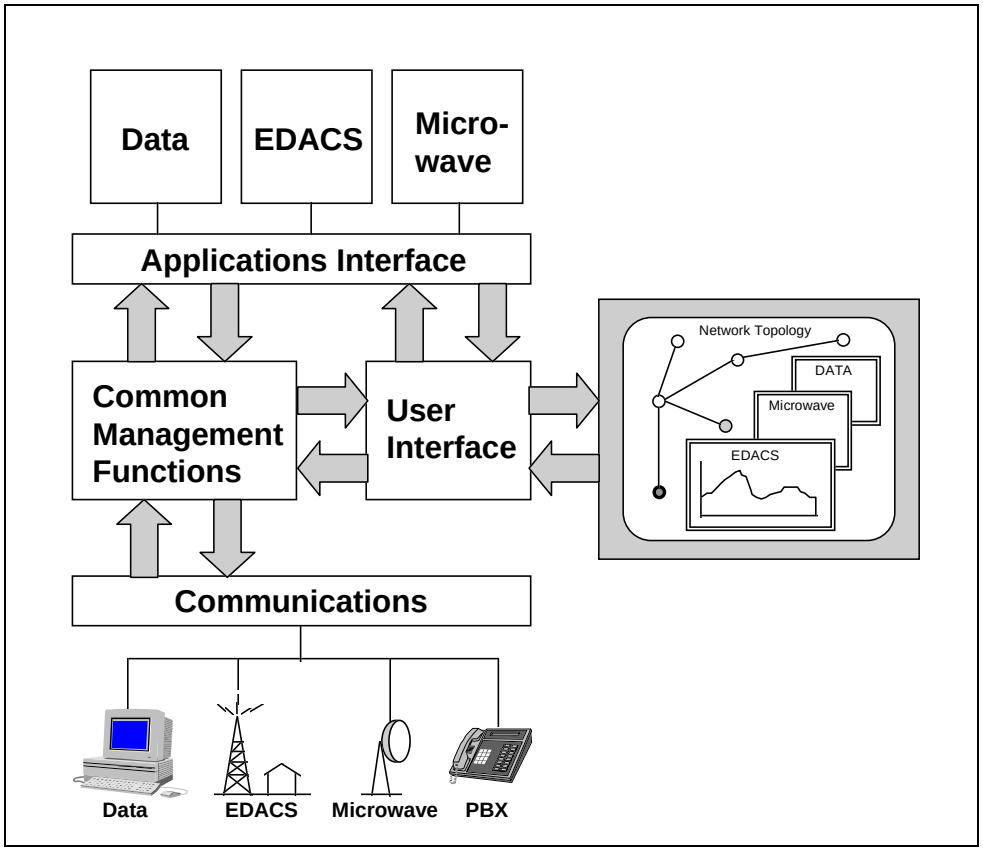


Figure 6 - Typical Network Management Platform

4.3.4 Platform Architecture

The main goal of Network Management is providing a central control point for EDACS networks. The EDACS Network Manager provides the centralized platform which consolidates the various user interfaces.

The EDACS Network Manager Application is based on the industry standard TCP/IP board protocols as shown in Figure 7. The Network Manager platform architecture is as follows:

- Performance Graphs -- EDACS application which interfaces with the OpenView database via the OpenView API and invokes 2-dimensional line graphs using the *xnmgraph* utility.
- Fault Management -- EDACS application which interfaces with the OpenView SNMP interface via its API and associates trap events with icons and other features.
- Map Generation -- EDACS application used to set up EDACS maps which interface with the OpenView database via the OpenView API and registration files and communicates EDACS element adds and deletes to Fault Management via the OpenView SNMP API.
- Real-time Monitoring -- The Multisite Monitor and Site Monitor are X Windows Motif UNIX applications.
- Menu Items -- EDACS application which interfaces with the OpenView Menu bar via registration files to realize the menu items.
- CEC/IMC Manager HP-UX Client -- EDACS application which communicates with the CEC/IMC Manager remote server using Remote Procedure Calls.

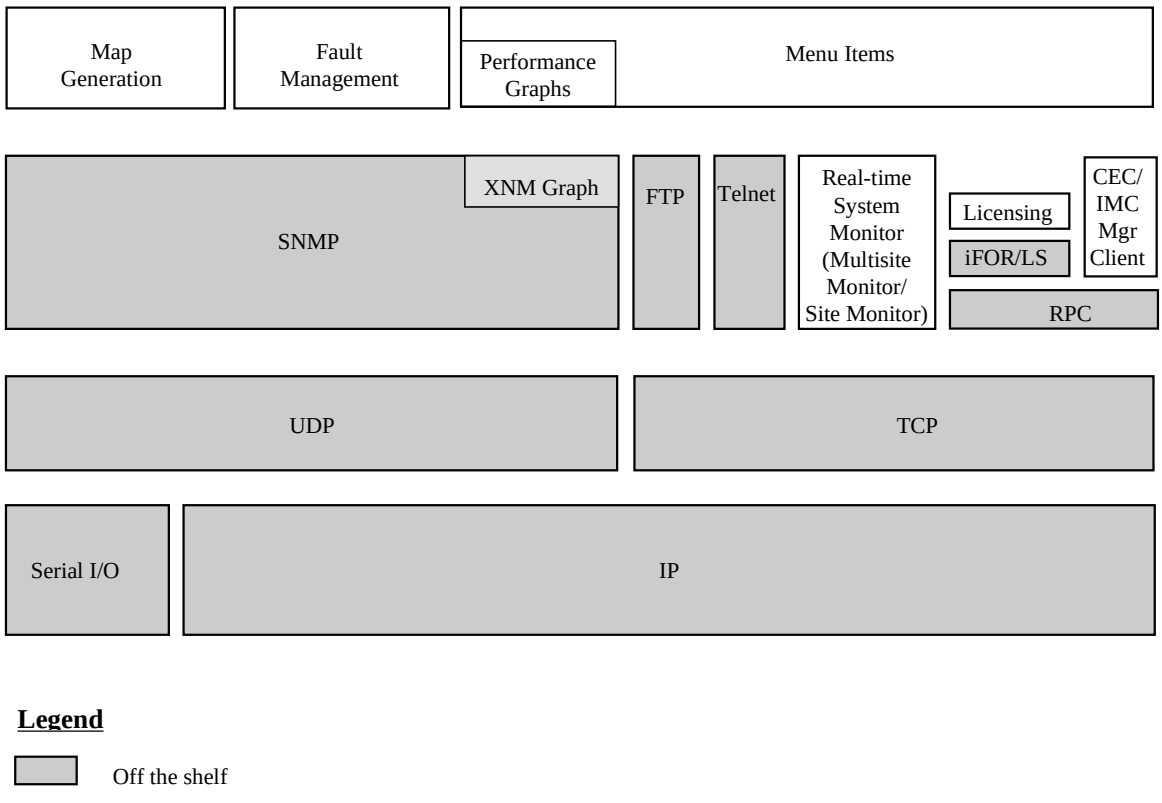


Figure 7 - EDACS Network Manager Application Architecture

4.3.5 Modem Access

Remote access using a modem permits the following:

- Access to the Network Manager application from a remote location.
- A means of troubleshooting or configuring the EDACS network from a remote location
- Direct access to the Network Manager in the event the LAN is inoperable.

Modem access directly to the Network Manager has the added feature that compression is possible. Xremote runs on the UNIX platform while PC-Xware runs on a PC.

Modem access to the LAN is possible via a Terminal Server with modem interface. However, this method may be slowed due to the graphical nature of the interface.

4.3.6 Log Maintenance

No log maintenance is required as the logs are self maintaining.

4.3.6.1 EDACS NM Application Log

Events from the EDACS NM application are written to **/usr/EDACS/logs/edacs.log**. This file contains messages regarding unexpected behavior and should be viewed on a periodic basis. Normally, the file does not grow very quickly. This file is capped at 1 Megabyte. When the file reaches 1 Megabyte, it will be copied to **edacs.log.old** and a new file will be opened.

4.3.6.2 Trap Log

All received event entries that have been configured to be logged are written to **/usr/OV/log/trapd.log**. The file may consume memory quickly. To enable archiving, or to minimize disk space usage, remove older entries from the log file. These removed entries may be stored in a separate file, or deleted entirely. The size of the file is based on the number of events. By default, the log file holds 3500 events. If the maximum number of events is exceeded, the log file is renamed with an "**.old**" extension and a new log is opened. Searching the alarms log will traverse the current and the "**.old**" logs.

NOTE

The **.old** log will be overwritten once the current log is full.

4.4 HIERARCHY OF MAP LEVELS AND ICONS

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

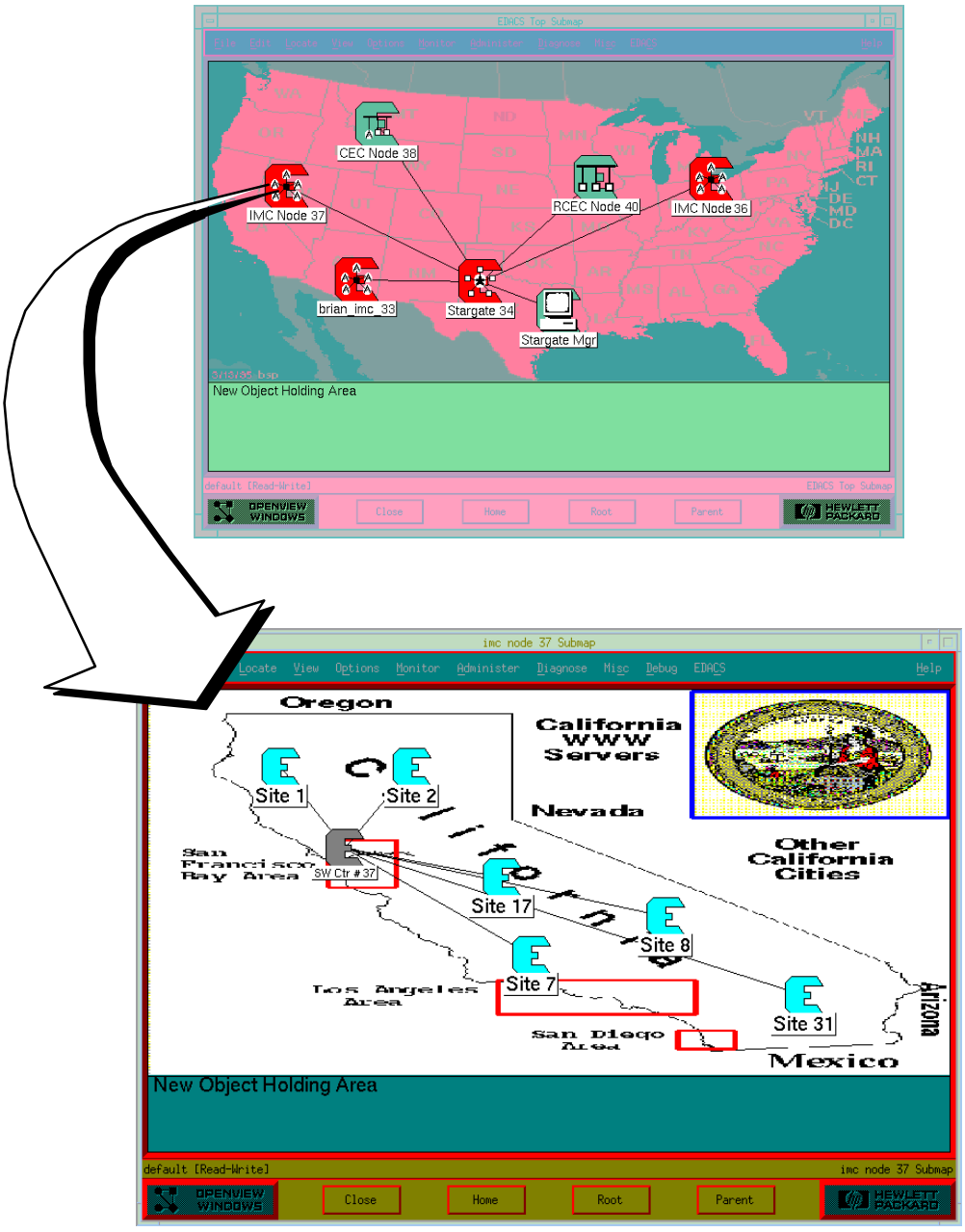
Four network levels are suggested: EDACS, Multi-Node, Node, and Site. However, there are no restrictions regarding placement of EDACS icons on maps. Thus, all icons could be on one submap if desired. For customers without all the network levels listed above, the EDACS icon will explode into the first 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 Example Map Traversal Screens in this section.

A new term "Switching Center" has been added. 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 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.

4.4.1 Example 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.

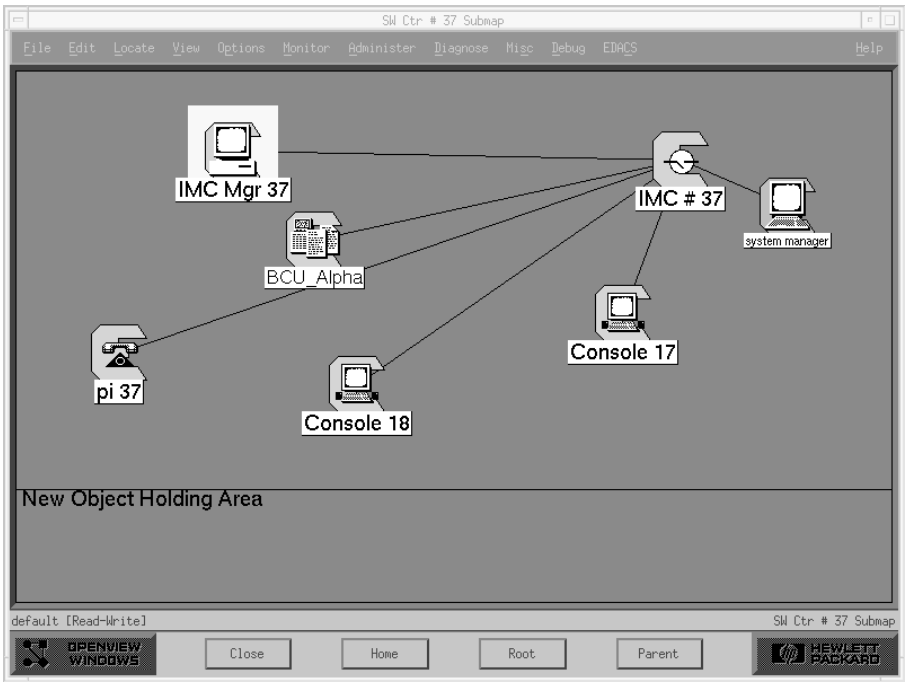
Exploding the EDACS icon  brings up a screen similar to that shown below.



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

Figure 8 - 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.

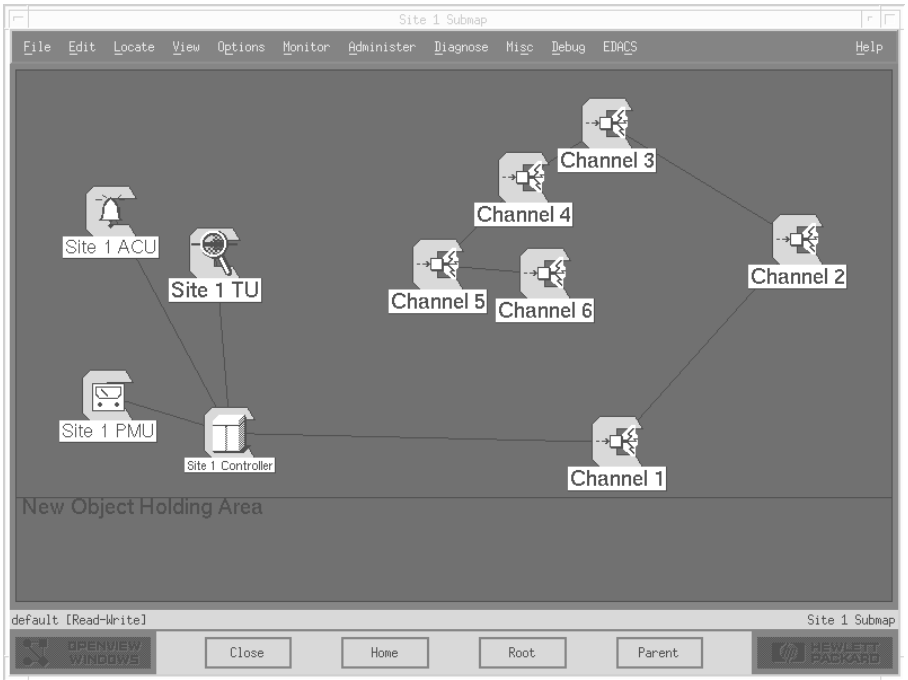


Figure 9 - Example of Exploding a Switching Center and Site Icon

5. 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 a valid icon is not selected, the EDACS menu option will be grayed out, meaning that it is inaccessible. Figure 10 shows the initial set of submenus which include Faults, Configuration, Accounting, Performance, and Software Version. Refer to the following text for additional details on each EDACS menu option.

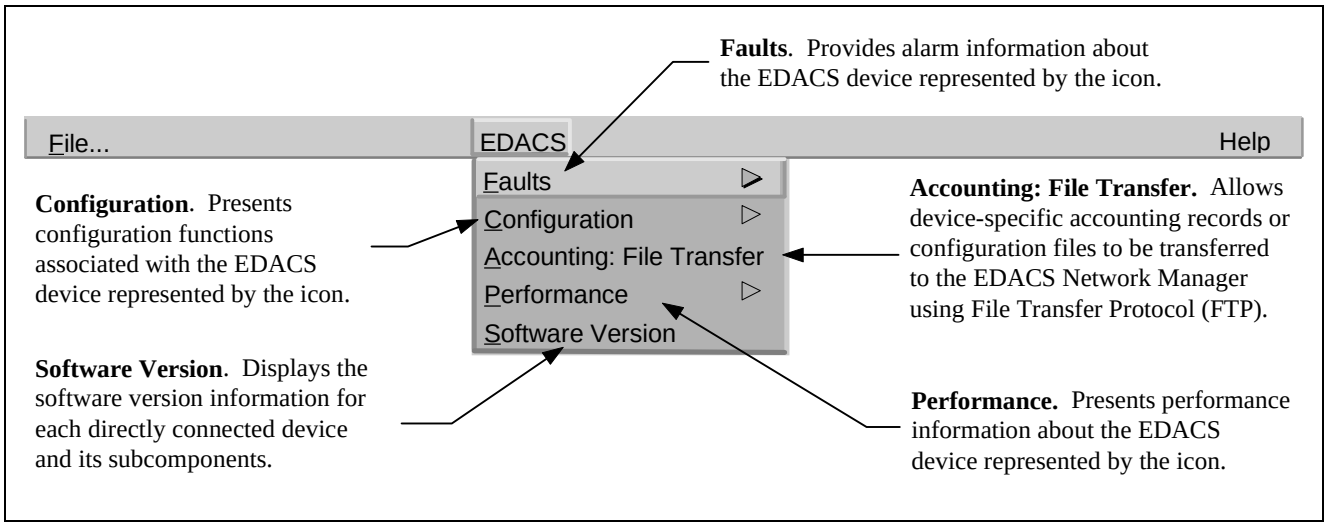


Figure 10 - EDACS Menu on Main Menu Bar

5.1 SOFTWARE VERSION

All software versions for the directly connected device and its subcomponents are listed as available. 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 11. The IP Address or host name of the directly connected EDACS device is listed in the IP Address field.

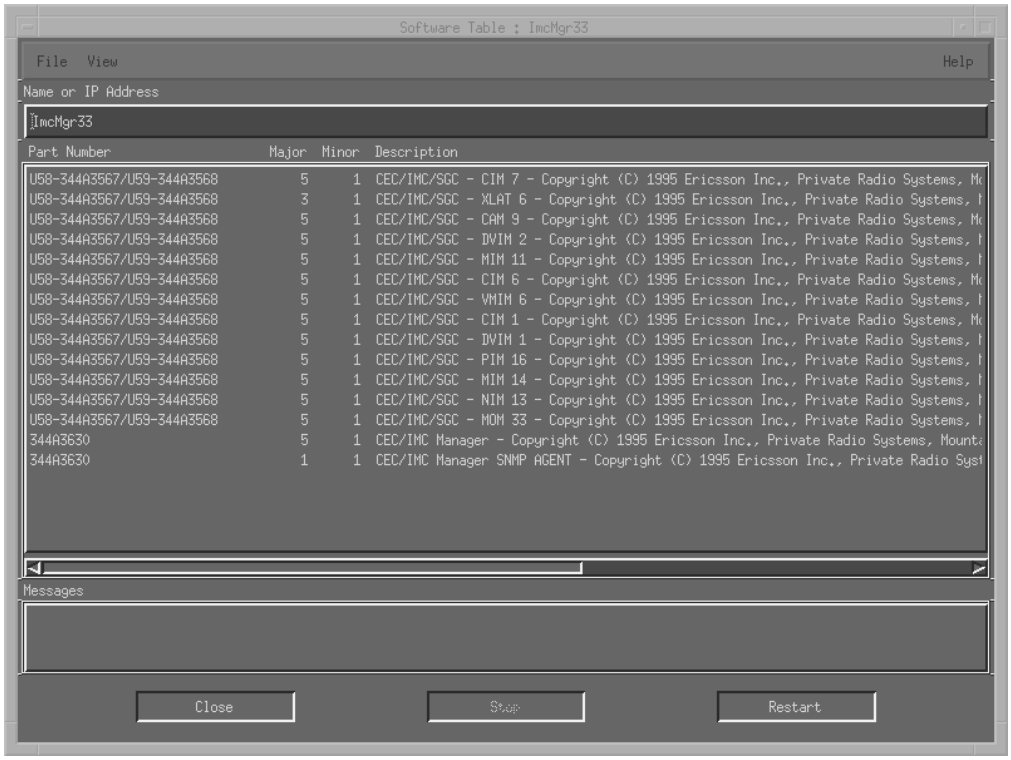


Figure 11 - Software Version Screen Example

5.2 HELP

EDACS Help has been integrated into the OpenView Network Node Manager Help system.

5.2.1 Menu Items

EDACS Help items are preceded with “EDACS” to make them easily identifiable. Help->Display->Legend includes the EDACS icons as well as the color associations. Help->Index->Application lists the EDACS applications and provides brief descriptions while Help->Index->Tasks lists the EDACS menu bar and Map Generation Help files.

5.2.2 Alarm

Alarm Help is integrated with the Event Browser and Event Configuration for easy access and tailoring. To invoke Alarm Help, select the event in the Event Browser and select the View->Description menu item.

5.3 EDACS FAULT MENU ITEMS

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

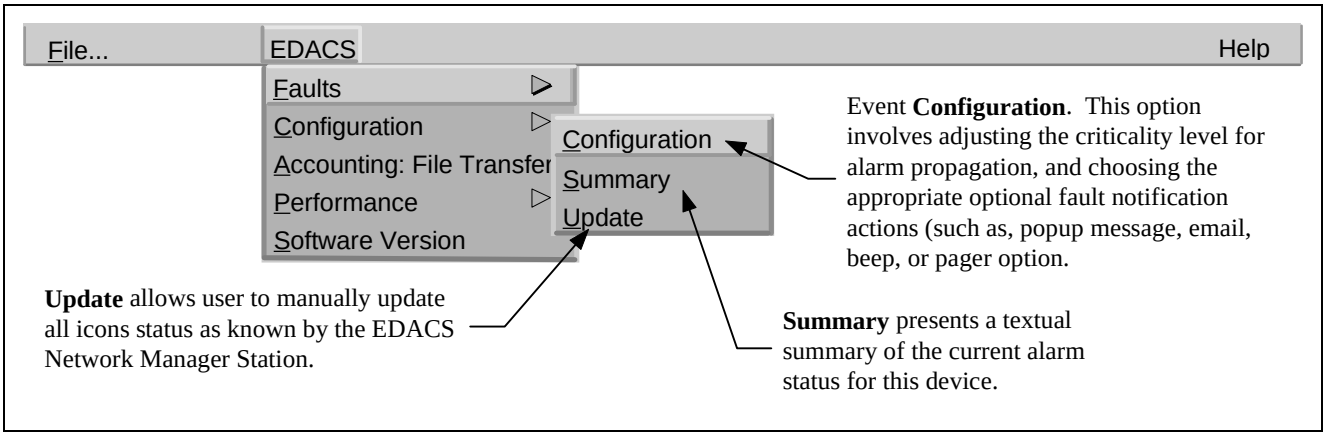


Figure 12 - EDACS Fault Menu

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

- **Normal**
- **Warning**
- **Minor**
- **Major**
- **Critical**

Each level has an associated display color to be used to update map objects (see Table 5). Upon receipt of the alarm, the color of the EDACS icon the alarm is against is set to the highest level alarm in existence for that icon. This color is also propagated up to all parent objects in upper-level maps. Table 5 contains the levels, descriptions, and associated colors. The levels and colors chosen are in accordance with HP OpenView Network Node Manager. 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.

EDACS 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 for actual fault items and Table 5 for the meaning of icon colors.

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 using File->Describe/Modify Map. This menu item generates a popup with an associated help button.

5.3.1 Fault Summary

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. One-shot events, such as “device Rebooted,” may have a popup associated with them. For a given map object, the EDACS NM can display the current alarms affecting icon color for that object. The display is in a short report (list) format, with each entry in the report listing the alarm, severity level, and time stamp the event was received. Detailed information is stored in the Event Browser.

Table 5 - 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

5.3.2 Fault Configuration

This menu item will bring up the OpenView Network Node Manager Event Configuration Window which allows actions and popup windows to be associated with events, and modifications of the category and severity level. This item does not configure threshold-oriented alarms. The Options -> Data Collection menu item is used for configuring threshold-oriented traps at the EDACS NM. Threshold-oriented traps at the remote element may be configured using the MIB Browser.

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

- 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.

5.3.3 Fault Update

This menu item updates all EDACS managed icons with the status as known by the EDACS Network Manager. When an icon transitions from unmanaged to managed, this menu item must be used to update icon status.

5.4 EDACS CONFIGURATION MENU

The EDACS Configuration MenuConfiguration 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 perform native configuration.
- **Reboot**: Automatically reboots the EDACS device.
- **Restart**: Restarts traffic after a shutdown.
- **Shutdown**: Shuts down traffic without losing connectivity.

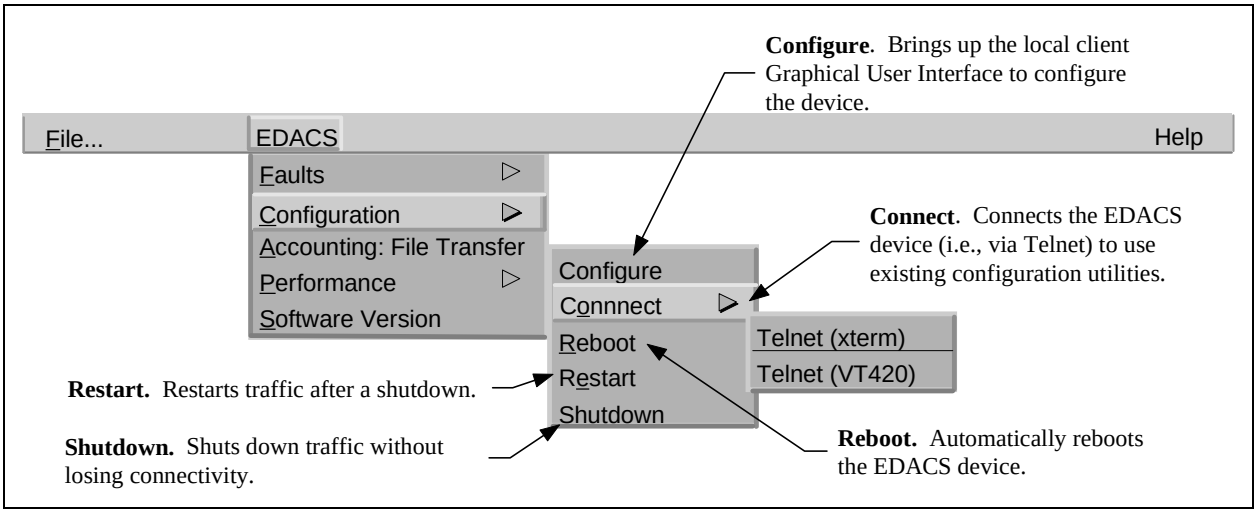


Figure 13 - EDACS Configuration Menu

5.4.1 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.

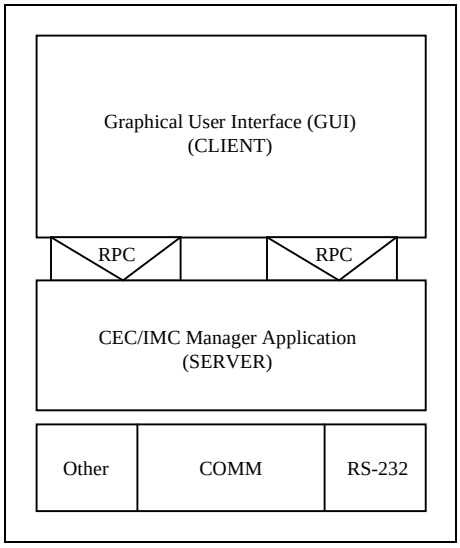


Figure 14 - CEC/IMC Client-Server Paradigm

5.4.1.1 Sample CEC/IMC Manager Screens

Some sample CEC/IMC Manager screens for configuration follow.

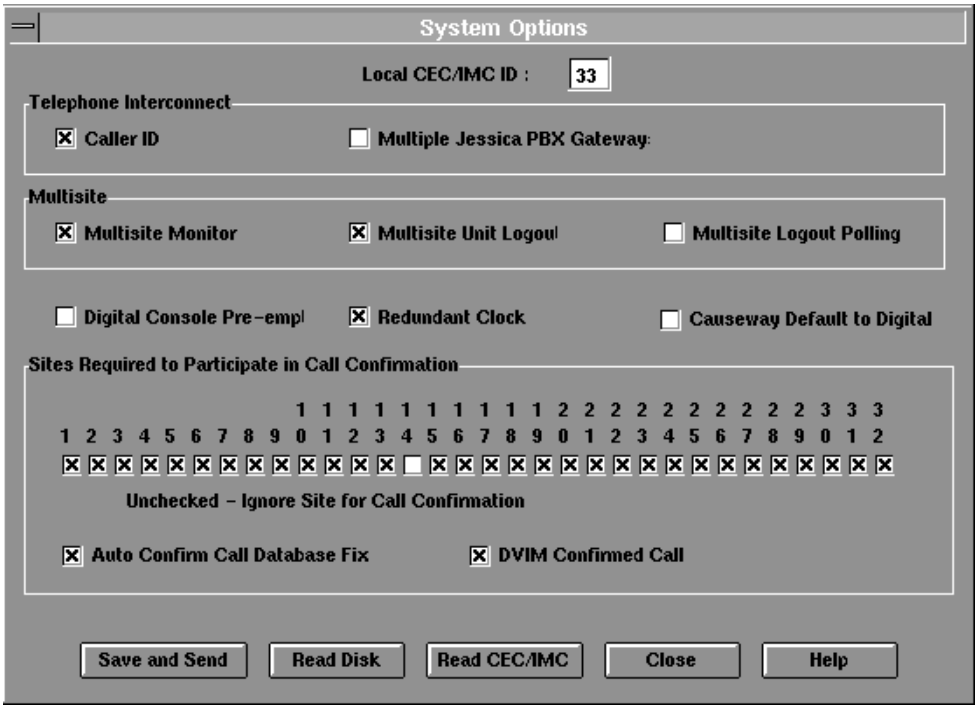


Figure 15 - System Options for Digital Console Pre-empt Example Screen

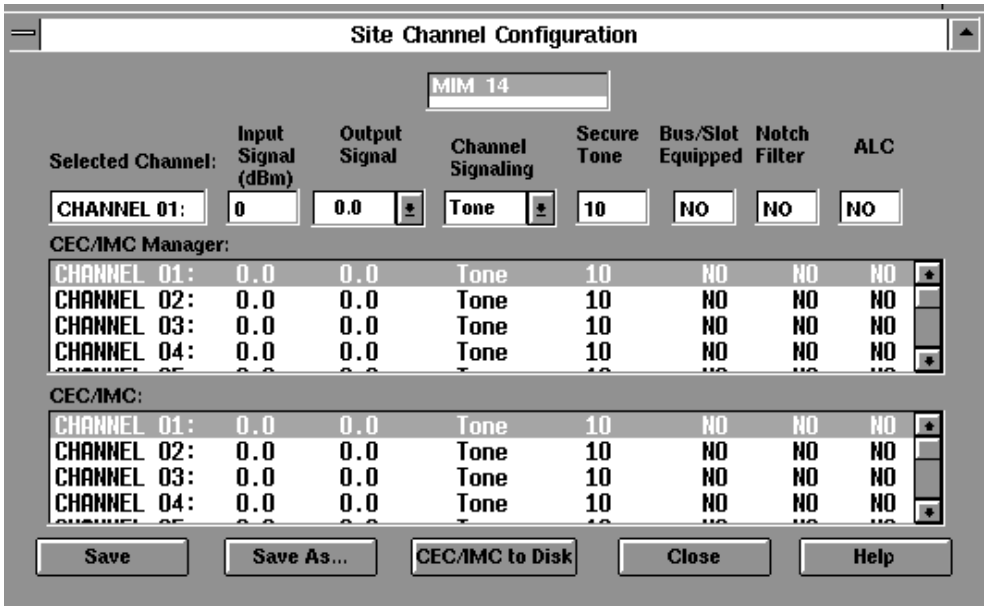


Figure 16 - Site Channel Configuration Example Screen

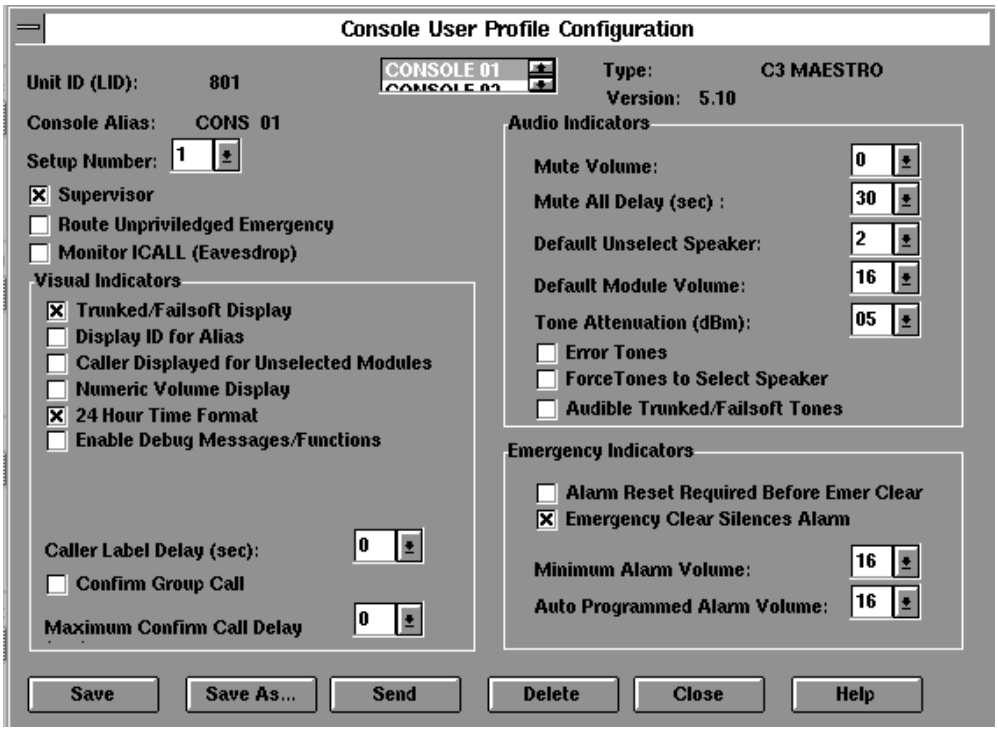


Figure 17 - Console User Profile Configuration Example Screen

5.4.2 Telnet Sessions to the PI, BCU, CAL, EDG, and System Manager

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. Telneting to the System Manager uses VT220 emulation because it is a VAX/VMS system running a screen-oriented application.

5.4.3 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 information is written to the same file displayed by the Event Browser. **NOTE:** User actions can be disabled at the remote platform.

5.5 ACCOUNTING: FILE TRANSFER MENU

Connects to the EDACS device via File Transfer Protocol (FTP) to allow device-specific accounting records to be transferred to the EDACS Network Manager. Configuration files may be transferred to and from the remote device for editing on the Network Manager platform.

5.6 EDACS PERFORMANCE MENU

The EDACS Performance Menu presents performance information about the EDACS device represented by the icon.

- **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.
- **Monitor**: Invokes Site Monitor and Multisite Monitor.

NOTE: In the Performance menu items shown below the choices for node and site are the same; therefore, only the node path is shown. Descriptions of menu items follow.

NOTE

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

The EDACS Network Manager Performance menu provides Two Dimensional Line graphs that measure the overall node and site level performance via various predefined groupings of performance parameters. The Performance menu also provides the interface to the Multisite Monitor and Site Monitor features.

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.

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 2D line graphs (summarizes traffic at a node) and site level 2D 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.

5.6.1.1 Line Graph Example

The example of a line graph, shown in Figure 18, 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.

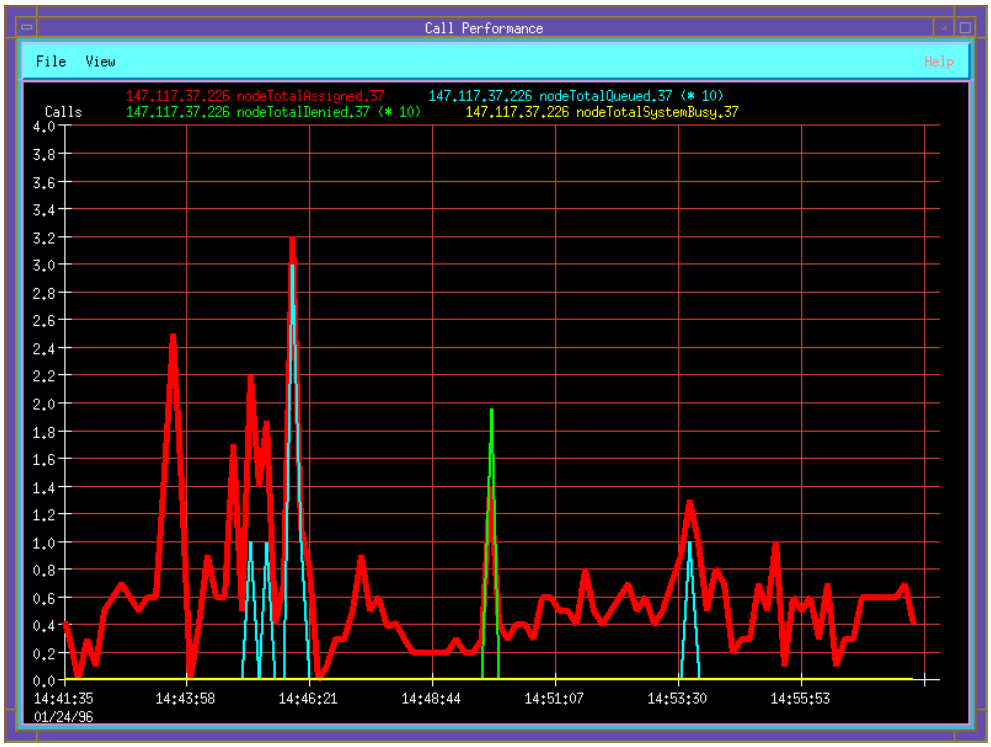


Figure 18 - Example of a Two Dimensional Line Graph

5.6.1.2 Customizing Line Graphs

When a performance item is selected from the Main Menu, a default Two Dimensional 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.

5.6.2 Performance - Utilization Sub-bar

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

The entries on the Performance sub-bar, see Figure 19, 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.

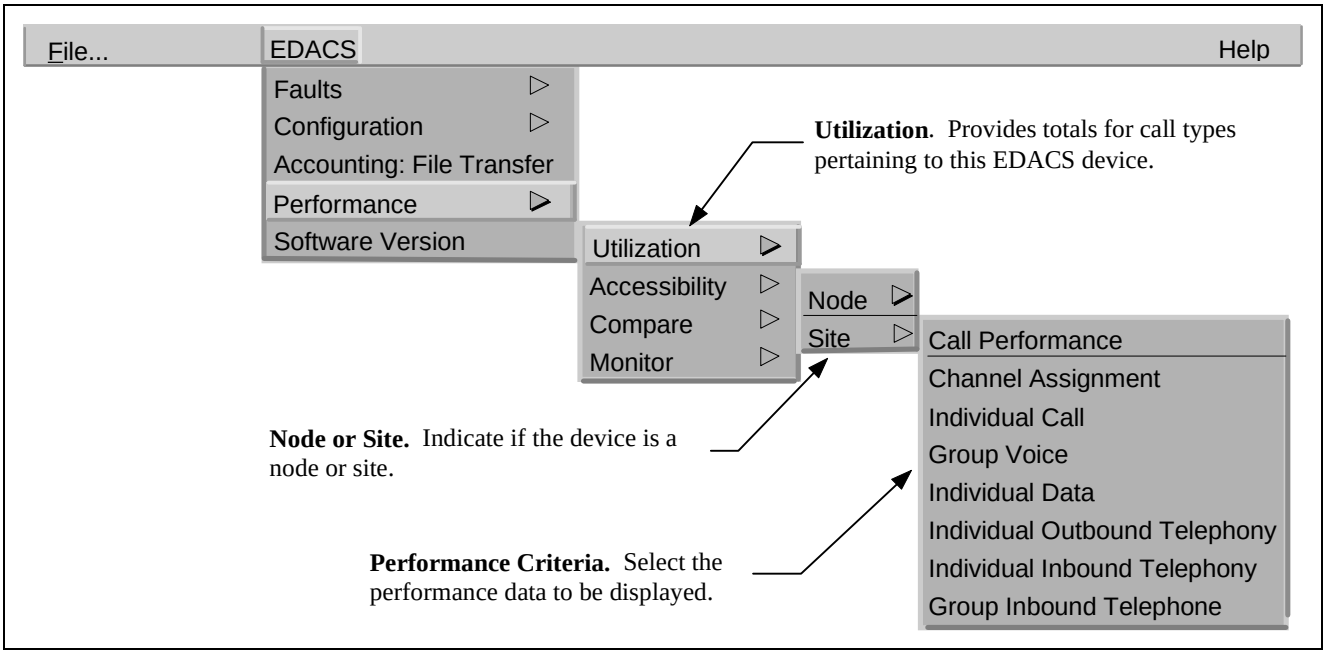


Figure 19 - EDACS Performance / Utilization Menu

5.6.3 Performance - Accessibility Sub-bar

The Performance - Accessibility menu 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.

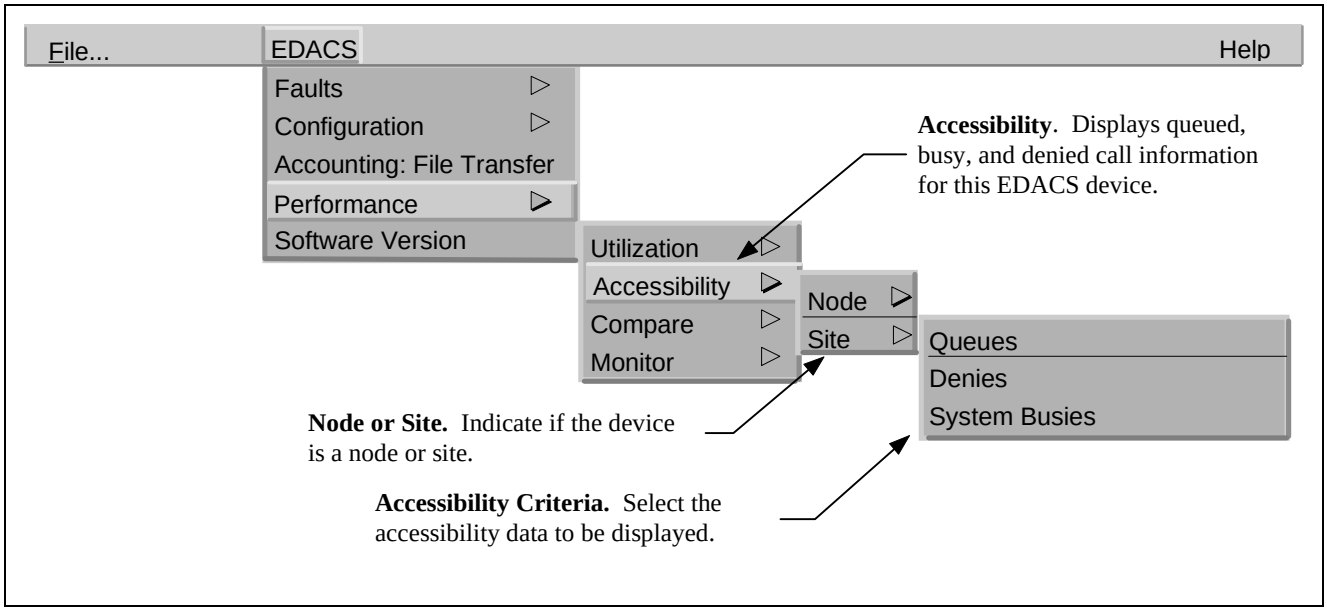


Figure 20 - EDACS Performance / Accessibility Menu

5.6.4 Performance - Compare Sub-bar

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

The following graphs will display a single MIB value 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.

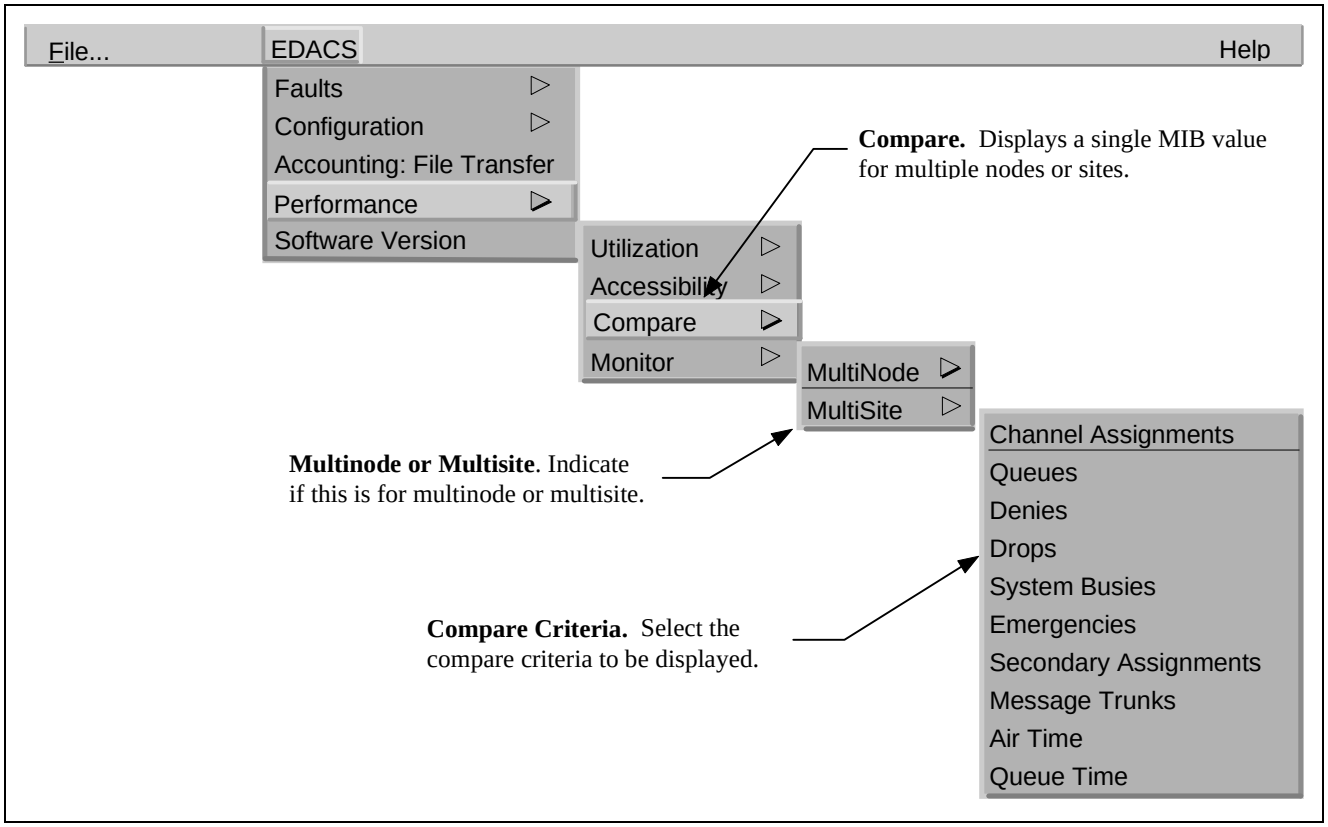


Figure 21 - EDACS Performance / Compare Menu

5.6.5 Performance - Monitor Sub-bar

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, 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.

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.

5.6.5.1 Monitor Invocation

Invokes a Multisite Monitor or Site Monitor session 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.

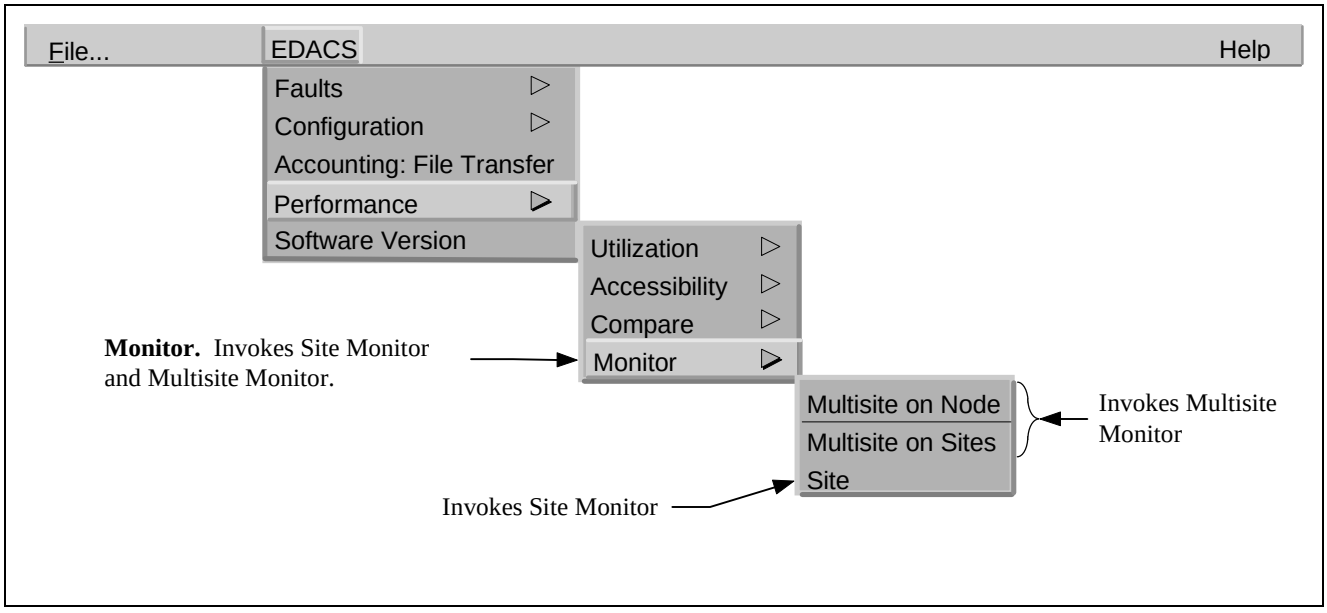


Figure 22 - EDACS Performance / Monitor Menu

5.7 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.

The main menu bar located at the top of the window contains three entries (refer to Figure 23): 1) File, 2) Options, and 3) Help. The File menu has only one option: Exit. The Exit button terminates the MSM application.

The Options menu has four options: Traffic Filter, Legend, Statistics Rows, and Quiet Drops. The Options menu is discussed in the next section.

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.

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. 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. For Multisite Monitor internodal 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. For multinode traffic, the MSM uses the Network Number to display a column for each IMC, StarGate, CEC, and Remote CEC. 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.

Vertical and horizontal scroll bars are generated automatically, as needed, for the work area.

Figure 24 shows an example of a typical Multisite Monitor screen.

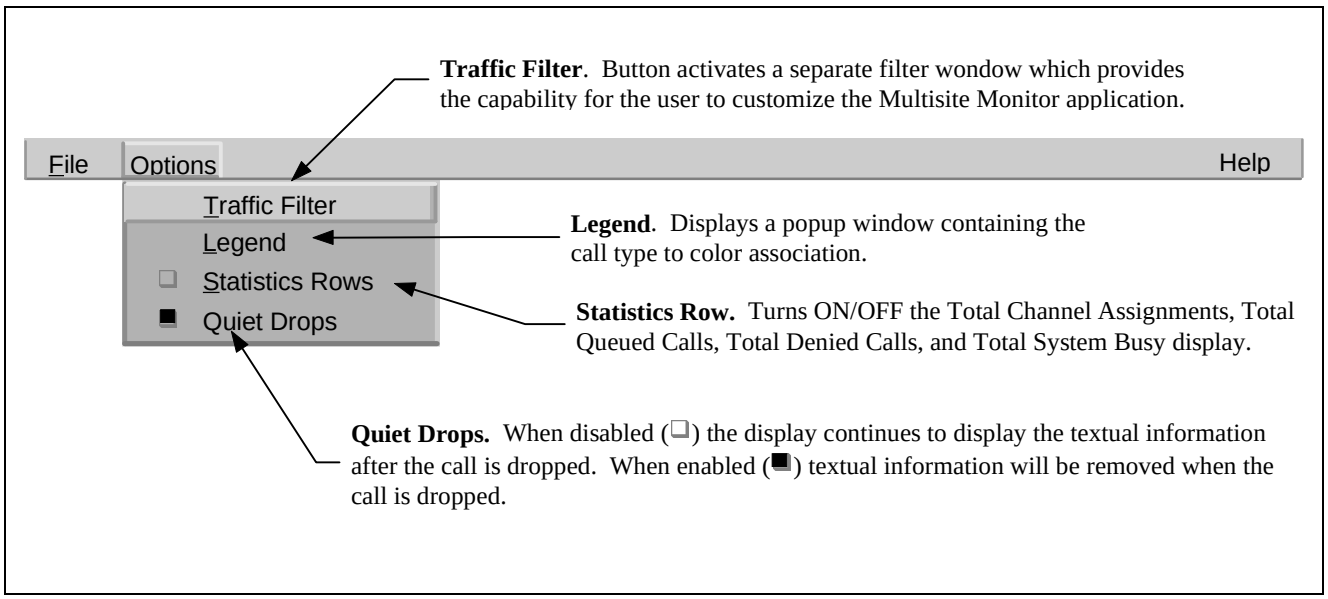


Figure 23 - Multisite Monitor Menu Bar

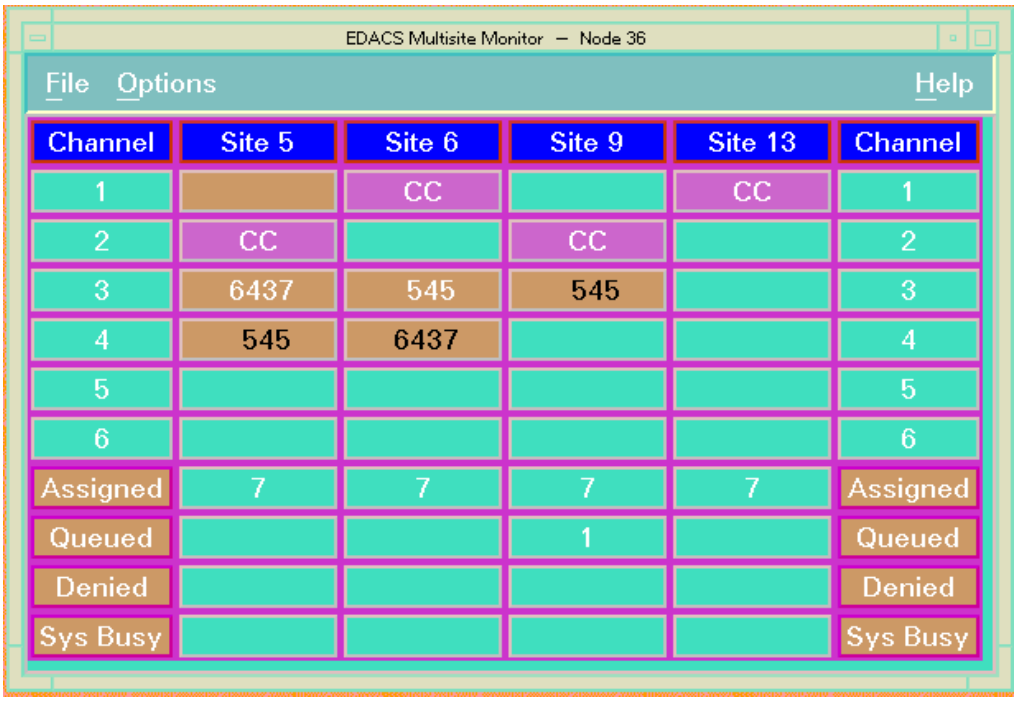


Figure 24 - Multisite Monitor Display Example

5.7.1 Special Features

The Options menu provides the capability for the user to customize the Multisite Monitor application to suit particular needs. The Options menu contains four options: Traffic Filter, Legend, Statistics Rows, and Quiet Drops.

5.7.1.1 Traffic Filter

The Traffic Filter button activates a separate filter window as depicted in Figure 25. 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.

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.

Figure 25 - Traffic Filter Window

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.

5.7.1.2 Legend

The Legend window activates a small window that serves as a key for the current Traffic Filter settings (see Figure 26). 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

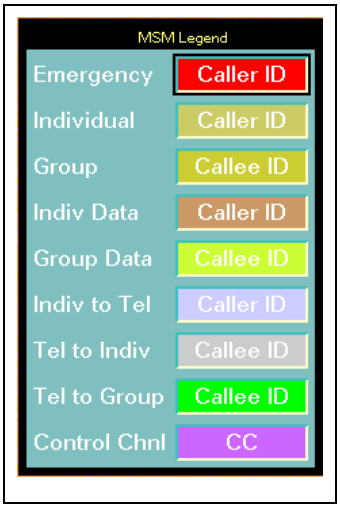


Figure 26 - Multisite Monitor Legend

chosen filter text. No modifications can be made to the filter settings via the Legend window. The window is for informational purposes only.

5.7.1.3 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 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.

5.7.1.4 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.

5.8 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 27). All windows can be manipulated (i.e., resized, iconized, closed) via standard window border operations.

The main menu bar located at the top of the window contains three entries: 1) File, 2) Options, and 3) 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. The Options menu is discussed in the next section. 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. Refer to the diagram below. These menu options may be selected via the mouse or keyboard mnemonics.

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.

5.8.1 Special Features

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

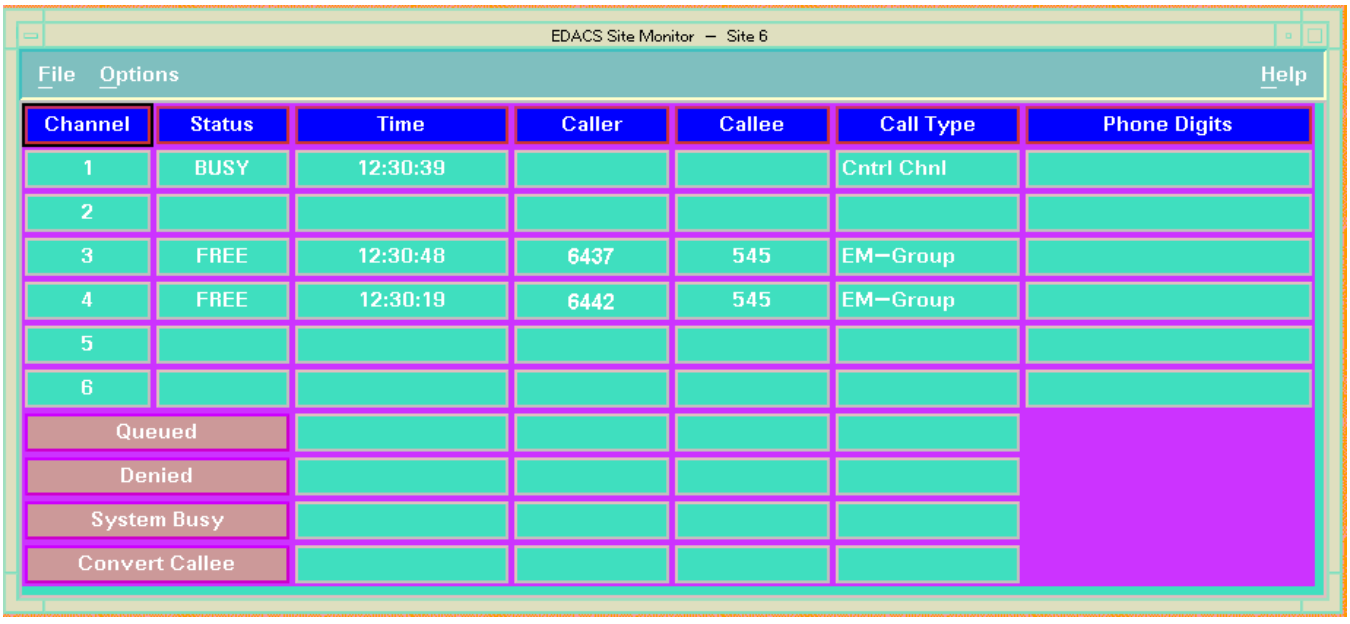


Figure 27 - Site Monitor Display Example

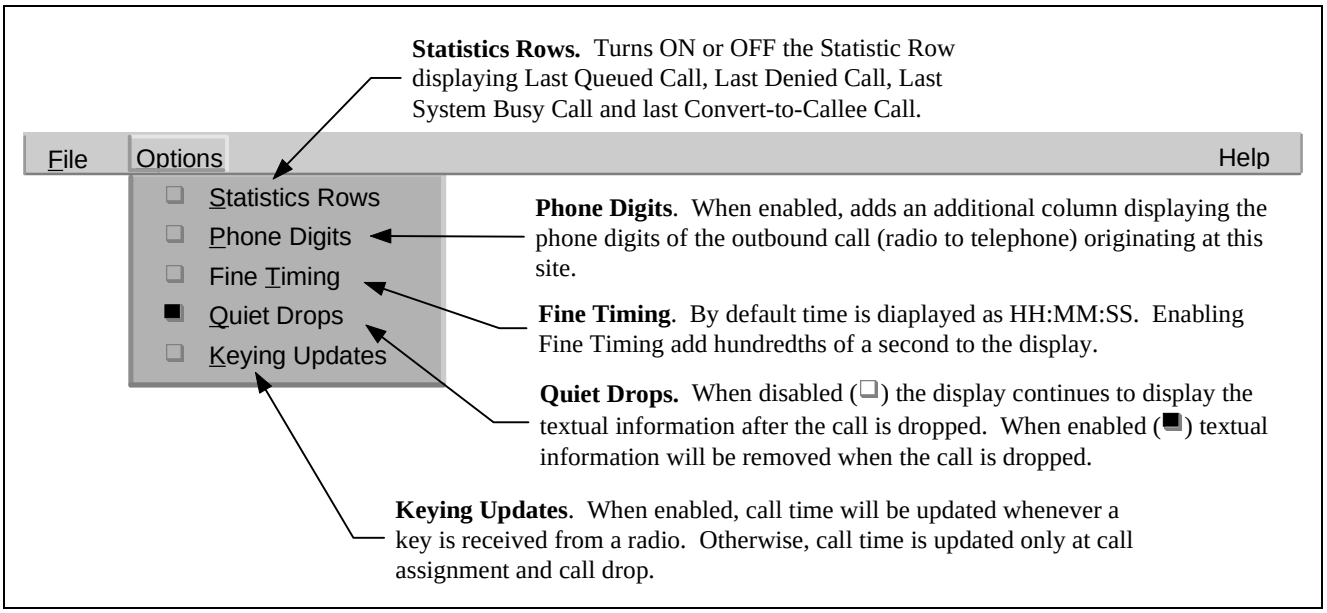


Figure 28 - Site Monitor Menu Bar

5.8.1.1 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.

5.8.1.2 Phone Digits

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.

5.8.1.3 Fine Timing

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.

5.8.1.4 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.

5.8.1.5 Keying Updates

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.

6. EDACS MAP GENERATION/PROPAGATION

The EDACS Map Generation application aids the generation of EDACS network maps. Hierarchical graphical maps representing the EDACS network are automatically generated based on data entered in the "EDACS Map Generation" attribute section of the popup window. The popup window appears when the following symbols are dragged onto the OpenView Network Node Manager map:

- IMC Node
- CEC Node
- Remote CEC Node
- Site
- Switching Center.

All other EDACS "symbol adds" will prompt for the identifiers required to uniquely identify them in the "EDACS Map Generation" attribute section of the popup window, except the EDACS Region Object. The "EDACS Region adds" only creates a submap.

The EDACS Map Generation attribute section of the popup associated with the "EDACS Top Icon add" specifies the clock and device polling intervals. All submaps are created such that the icons may be moved freely about the map.

The following configuration rules apply to the application. Violations of these rules will result in unmanaged elements; however, the icons will be allowed.

- Each CEC/IMC may have 30 consoles.
- A Remote CEC may have 0 sites.
- A CEC may have 1 site.
- An IMC may have more than 1 site.
- A StarGate may have 0 sites.

When certain EDACS icons are added to a map, the EDACS Map Generation application appears in the Attributes section of the OpenView Add Object popup. The EDACS icons with associated EDACS Map Generation Actions are listed below.

- **IMC Node Add** -- This operation displays a popup window asking how many channels to add on which sites and which consoles are present. It creates an IMC Node submap with Site icons connected to a Switching Center icon. It creates a Switching Center submap with Consoles connected to an IMC. It creates Site submaps with a Site Controller, ACU, PMU, TU, and the number of channels indicated in the popup.
- **CEC Node Add** -- This operation displays a popup window asking how many channels to add on which sites and which consoles are present. Note that a CEC supports one Site. It creates a CEC Node submap with Site icons connected to a CEC icon. It creates a Site submap with a Site Controller, ACU, PMU, TU, and the number of channels indicated in the popup.
- **Site Add** -- This operation displays a popup window asking how many channels to add on this Site. It creates a Site submap with a Site Controller, ACU, PMU, TU, and the number of channels indicated in the popup.
- **Switching Center Add** -- This operation displays a popup window asking which consoles are present. It creates a Switching Center submap with Console icons connected to an IMC.
- **EDACS Top Add** -- This operation displays a popup asking for the EDACS device polling interval and the EDACS clock synchronization polling interval.

- **Directly Connected EDACS Element Add** -- When an EDACS icon is manually added for a directly connected EDACS element, the Selection Name must equal the IP Address of the element or the host name as specified in /etc/hosts. The following are directly connected EDACS elements: **PI, BCU/CAL, CEC/IMC Manager, and System Manager**. The Selection Name ties the EDACS icon with the EDACS capabilities to the object created by the OpenView IPMAP application, the HP application which finds devices supporting SNMP on the LAN. 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 we create is also used by IPMAP. Not only must the Selection Name equal the IP Address, but the IP Host Name must equal the actual 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. (For example, the IP interface group will have an associated icon.) The parent of this child submap is in the IPMAP submaps not the EDACS submaps. This feature can aid in network connection debugging. Namely, to see where this element is in the overall network, go into the Directly Connected Device's child map and select the "parent" button.

Furthermore, the EDACS Network Manager must uniquely identify the device in the EDACS network. The EDACS Network Manager classifies three types of devices: Node, Subnode, and Subsite.

The list below shows the breakdown of EDACS devices.

- Node devices are IMC, StarGate, CEC, CEC/IMC Manager, BCU/CAL, and System Manager.
- Subnode devices are Console, Site Controller, ELI, PI, ACU, EDG, PMU, and TU.
- Subsite devices are GETCs and Base Stations.

The Describe operation displays the Identifiers used by alarm processing and performance graph invocation. Refer to LBI-39171 - EDACS Network Management Installation and Technical Reference Manual and LBI-39169 - User’s Guide for more information on this operation. Procedures to add and delete symbols and add connections are also presented in these manuals.

7. OPENVIEW NETWORK NODE MANAGER FEATURES

Numerous features are described herein; this section briefly describes the feature and refers the reader to the HP **OpenView Network Node Manager User's Guide** for the exact procedure. It was our attempt to leverage OpenView Network Node Manager to the fullest extent to allow the 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.

7.1 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.

7.2 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 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.

7.3 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 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.

7.4 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 User's Guide section titled *Collecting MIB Data*.

7.5 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 User's Guide sections titled *Collecting MIB Data* and *Defining Thresholds.*

7.6 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 User's Guide section titled *Viewing Historical Trends*.

7.7 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.

7.8 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 User's Guide section titled *Defining Actions for Events*. **NOTE:** Updates of the EDACS application will overwrite the event description (connect) field.

7.9 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

NOTE

Background graphics may contain no more than eight (8) colors.

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.

7.10 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 User's Guide section titled *Taking Snapshots of the Map*.

NOTE

Snapshots may consume noticeable amounts of memory.

7.11 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.

7.12 INTERNATIONALIZATION

The HP OpenView Network Node Manager product is sold in English only; however, its software architecture does support the conversion to multiple languages via the UNIX Native Language Support (NLS) utility without recompiling the application code. International code sets for single and multi-byte character sets are supported. (Refer to the list below for the languages supported by the HP Visual User Environment.) OpenView Network Node Manager manuals are printed in English only and the OpenView NNM application is available in English and Japanese.

american	danish.iso88591	hebrew.iso88598	portuguese
american.iso88591	dutch	hungarian	portuguese.iso88591
arabic	dutch.iso88591	icelandic	POSIX
arabic-w	english	icelandic.iso88591	rumanian
arabic.iso88596	english.iso88591	italian	russian
bulgarian	finnish	italian.iso88591	serbocroatian
C	finnish.iso88591	japanese	slovene
c-french	french	japanese.euc	spanish
c-french.iso88591	french.iso88591	katakana	spanish.iso88591
chinese-s (simplified)	german	korean	swedish
chinese-t (traditional)	german.iso88591	n-computer	swedish.iso88591
chinese-t.big5	greek	norwegian	thai
czech	greek.iso88597	norwegian.iso88591	turkish
danish	hebrew	polish	turkish.iso88599

NLS contains an extensive set of tools and routines to accomplish internationalization. It allows one discrete program to "speak" in a variety of languages. NLS addresses an application's internal functions (such as sorting and character handling) and the user interface (which includes displayed messages, user inputs, and currency formats). It accounts for local customs and conventions (i.e., number format, currency information, date and time format, case shifting, and collation), which are set according to each language. The selection of a specific linguistic environment is defined via UNIX environment variables.

Each multi-language application consists of three parts:

1. A language-independent program.

2. Separate message catalogs for each supported language.

3. An assortment of language tables that contain language-specific information and conventions unique to a particular locale.

Because all language-dependent processing information is kept external to the program source, programmers need not modify or recompile the program source code to provide the application in another language. The language specification occurs at runtime.

The EDACS Network Manager Application also uses NLS. However, only English is currently supported. Translation efforts will be required to support other languages.

7.13 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 application. The user of the EDACS Network Manager can manually place icons from another application into EDACS NM maps or vice versa.

8. NETWORK PLANNING

Before a customer can install the Network Manager, it will be necessary to identify the system requirements and plan out the entire network. The following sections provide useful information for analyzing the user's requirements based on the amount of traffic and associated EDACS equipment interfacing with the Network Manager.

In addition, a Network Manager survey is included at the end of this manual. This survey should be completed by an Ericsson Systems Engineer during the planning phase of the Network Manager installation. The survey will enable the engineer to further define the user's system and obtain information necessary for configuring and customizing the system.

8.1 NETWORK TRAFFIC ANALYSIS

The following graph depicts the requirements on the network based on various polling intervals. In order to determine the amount of traffic generated by the EDACS Network Manager polling EDACS devices, the following assumptions were made:

- To retrieve one object, two network packets are required (i.e., one "get" packet and one "receive" packet).
- Each network packet consists of the following:

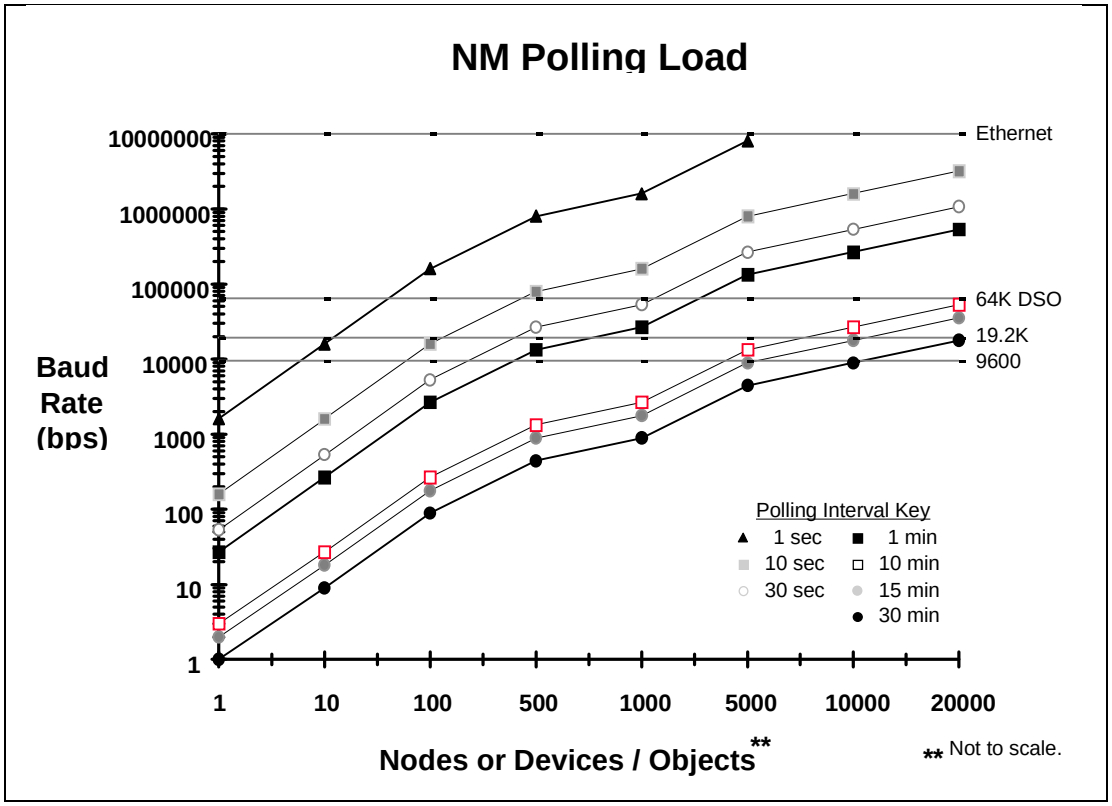
Ethernet header	14 bytes
IP header	20 bytes
UDP header	8 bytes

Figure 29 - Network Manager Polling Load Diagram

SNMP header and data packet	50 bytes min. (484 bytes max.)

In order to simplify the calculations, the network packet size is approximated at 100 bytes.

- Estimated Bandwidth Usage is as follows:



Multisite Monitor/Site Monitor per IMC connection

3600 calls/sec x 100 bytes/call = 360000 bytes/sec

2-dimensional Performance Graph with 1 parameter

200 bytes/interval x 0.1 intervals/sec = 20 bytes/sec

This approach can provide a first order level of traffic. Contact Systems Engineering for a more detailed analysis.

The following is an example of the Polling traffic analysis:

A 9600-baud connection is totally saturated when:

> 10 EDACS devices are being polled every second,

> 500 EDACS devices are being polled every minute, or

~ 10,000 EDACS devices are being polled every half hour.

8.2 LAN INSTALLATION

LAN installation is a non-trivial problem. Some of our customer base has LAN connectivity between the IMCs and a LAN support staff which will have a preference for how to connect our equipment into their network. At the other extreme, some customers will not have any LAN connectivity. The NM Survey at the end of this document is required to be filled out as early as the proposal stage.

A preliminary LAN analysis should be performed to determine whether the customer's proposed LAN connectivity solution is appropriate and to determine the need for a custom LAN solution.

EDACS devices are connected via a local LAN at each IMC, as shown in Figures 2 and 3. IMCs are also connected via a LAN. We recommend isolating our local LAN at each IMC from the customer's LAN

A few high level recommendations are presented below. These recommendations are intended to give a flavor of the choices. A preliminary LAN analysis is required to ensure proper LAN design.

8.2.1 Installing a New LAN

If there currently is not a LAN connection at IMC locations, and distance too great for an Ethernet LAN then a router may be used instead of a bridge. A router can convert from the Ethernet physical media to a T1 physical media. A leased T1 line could be run between the IMC locations.

8.2.2 Installing On An Existing LAN

It is recommended that a bridge router isolate the equipment located at each IMC such as the PI, BCU, EDG, or IMC Manager from the customer's network. A bridge may be programmed to restrict traffic flow based upon Media Access Control (MAC) address of devices, thus increasing security of remote access to EDACS devices. In addition, if the customer perceives our traffic is unduly loading his LAN, he has the ability to cutoff our traffic via the bridge to determine if whether we are the source of the LAN problem.

8.3 NETWORK IP ADDRESSES

Prior to configuring and installing the Network Manager, it is important to determine the IP Addresses that will be used to identify the various elements attached to the network.

The Network Management system uses a TCP/IP network consisting of multiple devices connected together. Each device on the network is assigned a unique internet or IP address. Therefore, the first step is to determine the IP Addresses that will be used.

IP Addresses are dependent on the class of the network. Network classification is described in the following sections.

8.3.1 IP Address Classification

Each host attached to the TCP/IP network is assigned a 32-bit address. Each address is a pair identifying the Network ID and the Host ID. The address assignments are developed according to the conventions for one of the five IP Address classes (A thru E). A Class A address partitions the 32-bit address into an 8-bit network portion and a 24-bit host portion. A Class B address partitions the 32-bits into a 16-bit network and 16-bit host partition. The Class C address partitions the address into a 24-bit network and 8-bit host portion. These addresses schemes can be used for any of the IP addresses. Class D and E addresses can not be used. Network Addresses must be unique and only be used once in an internet.

For ease of use, the 32-bit internet address is normally written using dotted decimal notation. This numbering system breaks up the four octets making up the IP Addresses are made up of separated by periods. For example, the IP address shown below is written in dotted decimal notation as follows:

10000000 00001010 00000010 00011110

dotted decimal notation = 128.10.2.30

The addresses can also be written in hexadecimal. Each octet can range from decimal 0 to 255 or hex 0x00 to 0xff.

The number of octets in each is based on the Class of the address. The Class of the address is determined by the value of the first octet as shown in Table 6.

Table 6 - IP Address Classification

CLASS	First Octet	Network ID Portion	Host ID Portion	Number of Host IDs
A	1-126	First octet	Last three octets	16M
B	128-191	First two octets	Last two octets	65K
C	192-223	First three octets	Last octet	254
D	224-239	N/A	N/A	N/A
E	240-255	N/A	N/A	N/A

Several conventions and special cases should be noted:

1. If the IP Address is all zeros, it refers to any host.
2. If the IP Address is all ones, the destination is all hosts on the local network.
3. If the Network ID is all zeros, the IP Address refers to a host on this network. This is only valid at system startup and is not a valid destination address.
4. If the Host ID is all zeros, the IP Address refers to the Network ID.
5. If the Host ID is all ones, the IP Address refers to all hosts on the specified network (not valid on the EDACS Network).
6. If the first octet is 127, then this is a local loop-back, normally used for testing and inter-process communication.
7. Class D addresses are multicast.
8. Class E addresses are reserved.

8.3.2 Ethernet Addresses

Ethernet Addresses are 64-bit addresses assigned by hardware vendors. Normally, an Ethernet Address is permanently assigned to a hardware device. The **A**ddress **R**esolution **P**rotocol (ARP) that is built into the Internet Protocol allows devices to query each other for their Ethernet Address. For these reasons, Ethernet Addresses are of minor importance when setting up a network, and are not discussed in detail.

A Network Address needs to be chosen for the EDACS Network. A Class C address typically isn't used since each radio must be assigned an address, and most EDACS Networks have more than 254 radios. A Class B address can be used to conserve Class A Network IDs.

If an EDACS system has no connections to another LAN, then we recommend using the default IP Addresses listed in Table 7.

Remember, since each network address must be unique, the IP Address assigned to the Network Manager must be reserved so it is not used any where else in the network.

8.3.3 Assigning Individual Addresses

After the Network Addresses have been decided upon, individual addresses within each network should be assigned. These addresses should be recorded on the Network Manager Survey forms.

For the EDACS Network, an IP address must be assigned to every LID and GID being used in the system.

The simplest way to map IP Addresses to LIDs is to map all of the LIDs to a block of IP Addresses in such a way that there is a one-to-one correspondence between the LIDs and the Host ID portion of the IP Addresses. Assuming the LIDs start at 64, the IP Addresses would start at 128.1.0.64. By allocating an IP Address for all possible LIDs now, future maintenance is reduced.

To compute the next available block of IP Addresses for the Groups, the Host ID portion of the IP Address of the highest LID (16382) can be converted to hex to get a value of 0x3ffe. Next, the octets can be individually converted back to decimal to get an IP Address of 63.254 (128.1.63.254). IP Address 128.1.64.0 can be used as the starting address for the GIDs to keep a one-to-one correspondence between the GIDs and the IP Addresses.

Table 7 - Recommended Default EDACS IP Addresses

SITE	EQUIPMENT	RANGE	IP ADDRESS
IMC 1	NETWORK IP	192.168.201.1 to 192.168.201.254	192.168.201.0
	IMC MGR		192.168.201.1
	NETWORK MANAGER		192.168.201.2
	SYSTEM MANAGER		192.168.201.10
	SMGDS 1		192.168.201.11
	SMGDS 2		192.168.201.12
	SMGDS 3		192.168.201.13
	SMGDS 4		192.168.201.14
	SMGDS 5		192.168.201.15
	BCU/CAL		192.168.201.20
	CAL TS 1		192.168.201.21
	CAL TS 2		192.168.201.22
	JESSICA PI		192.168.201.30
	JESSICA PI	Future	192.168.201.31
	EDG		192.168.201.40
	EDG		192.168.201.41
	PROFILE MGR		192.168.201.50
	STARGATE	If co-located	192.168.201.200
	HUB TERM SERVER		192.168.201.210
	CSU/DSU		192.168.201.220
	MUX/DACS		192.168.201.240
	UPS		192.168.201.241
	HUB		192.168.201.250
	HUB		192.168.201.251
	ROUTER		192.168.201.253
	ROUTER		192.168.201.254
STARGATE	NETWORK IP	192.168.200.1 to 192.168.200.254	192.168.200.0
	IMC MGR		192.168.200.1
	HUB		192.168.200.250
	ROUTER		192.168.200.254
IMC 2	NETWORK IP	192.168.202.1 to 192.168.202.254	192.168.202.0
IMC 3	NETWORK IP	192.168.203.1 to 192.168.203.254	192.168.203.0
to			
IMC 16	NETWORK IP	192.168.216.1 to 192.168.216.254	192.168.216.0

9. FCAPS

The International Organization for Standards (ISO) Network Management forum identifies five functional areas often referred to as "FCAPS." This model serves as the basis for the EDACS Network Management strategy. The five areas are as follows:

1. Fault Management
2. Configuration Management
3. Accounting Management
4. Performance Management
5. Security Management

Each directly connected Network Element platform within EDACS can be viewed as a communication device that should have

- FCAPS data stored in a standard format that can be queried by anyone.
- Hooks in applications that maintain the FCAPS data.
- A standard agent to communicate the FCAPS data.

The scope of the FCAPS areas and how each relates to EDACS follows.

9.1 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.

EDACS fault management employs two complementary methods for detecting that a fault has occurred:

- **Asynchronous Trap Handling**: All directly managed EDACS network devices generate events via SNMP traps. When an alarm condition occurs or when the alarm condition clears, the SNMP trap is triggered. The Network Element sends the trap data to the EDACS Network Manager. The Network Manager receives these traps and interprets them for updates to the appropriate map objects and performs any associated actions. Directly connected Network Elements can generate SNMP traps to up to five (5) IP Addresses.

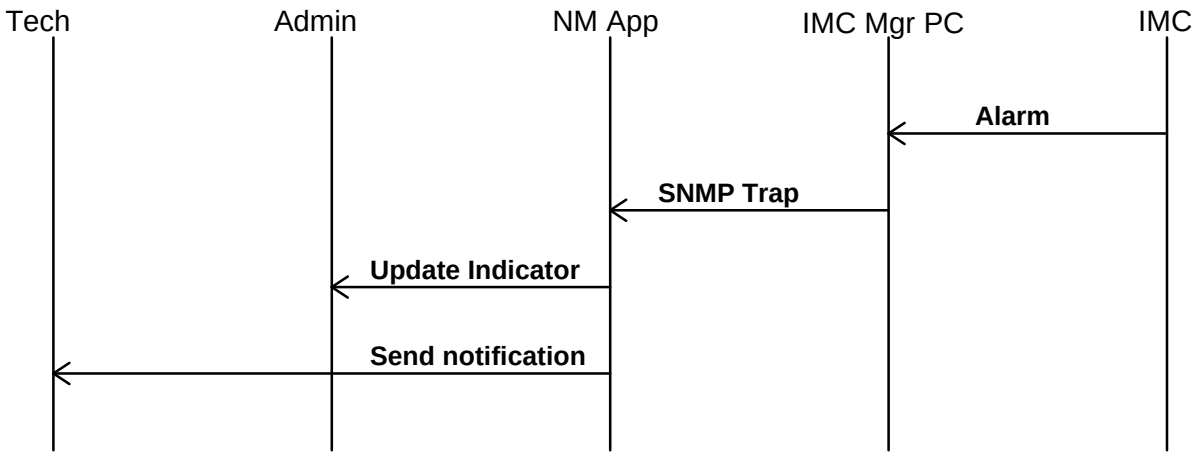
  Polling of Network Elements: Due to the unreliable nature of SNMP trap delivery, the EDACS Network Manager can periodically poll devices to ascertain the existence of a fault. It also polls to determine whether active faults have cleared. All enterprise traps have a readable Management Information Base (MIB) Object corresponding to the status of the trap events that the EDACS Network Manager can poll.

  The device polling interval is configurable through the EDACS Network Manager application. For more information, see LBI-39171, EDACS Network Management Installation and Technical Reference Manual.

  SNMP Agents can restrict the access to MIBs to read only, or read and write for specific IP Addresses with specific community names. An agent may also control which Network Manager station may manage it.

9.1.1 CEC/IMC Alarms

Alarm SET/RESET Use Case

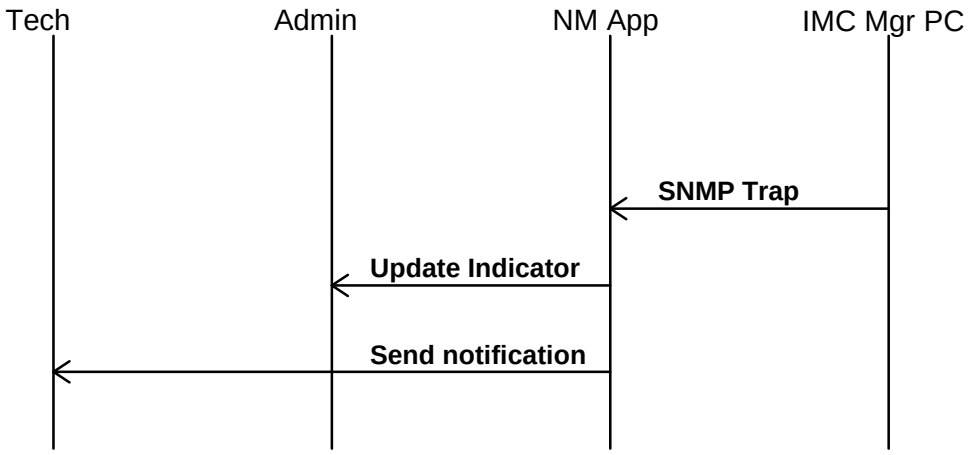


FAULT NAME	DESCRIPTION	SEVERITY LEVEL
CI_Clock_Bank_Fail	When a Controller board detects a Clock Failure, this trap is generated. If three of these traps are sent, a Clock Board Failure should also be sent.	**Major**
CI_Clock_Board_Fail	When three Clock Bank Failures occur, this trap is generated. A Clock Board Failure can disrupt audio on the entire node.	Minor
CI_GSC_Bus_Fail	The GSC bus is the main bus on the IMC. A GSC bus failure can disrupt audio on the entire node. This failure can be caused by an actual hardware failure, but the condition of the END NODE controller board should also be checked.	**Critical**
CI_HDLC_ChanA_Fail	HDLC Channel A Failures -- PIM-PI or CAM-to-PI control link.	**Major**
CI_HDLC_ChanB_Fail	HDLC Channel B Failures -- Controller-Audio Board link. An audio card has stopped responding. The Audio assignment indicates which audio card has stopped responding. The controller card involved is indicated by the Controller Assignment.	**Major**
CI_NIM_Link_Fail	Network Interface Module (NIM) (Radio Switch to Radio Switch) link failures. This failure can be caused by the local NIM or the Far End NIM.	**Major**
CI_MIM_Link_Fail	MASTR II/III Interface Module (MIM) (Radio Switch to Site) link failures. Usually this error is caused by the physical link between the IMC and the Site. In the case of T1/E1, check for excessive frame slips or Fsync errors that may be causing the condition.	**Major**

FAULT NAME	DESCRIPTION	SEVERITY LEVEL
CI_CIM_Link_Fail	Dispatch Console Interface Module (CIM) link failures.	**Major**
CI_PIM_Link_Fail	Jessica Private Branch Exchange Interface (PIM) link failures.	**Major**
CI_VMIM_Link_Fail	Conventional Virtual MASTR II/III Interface Module (VMIM) link failures.	**Major**
CI_MIM_Ctrl_Mismatch	Mismatch of MIM and Site assignment. Either the Site or the MIM has been set to an incorrect assignment. MIM assignments are selected at the Dip Switch Settings. Both the MIM and the Site must have the same assignment value. **NOTE:** This event does not affect icon color.	Warning
CI_PIM_Ctrl_Mismatch	Mismatch of PIM and Jessica Private Branch Exchange Interface (PI) Site assignment. Both the PI and the PIM must have the same assignment. **NOTE:** This event does not affect icon color.	**Major**
CI_Multi_End_Nodes	Multiple End Nodes set on the IMC GSC bus. **NOTE:** This event does not affect icon color.	**Major**
CI_DS1_Trunk_Fail	DS1 trunk failure. If this error occurs, it is probably due to configuration errors in the T1/E1 setup at the CEC/IMC Manager. Check the configuration first and then check the physical link.	**Major**
CI_Failsoft_Site	MIM has detected that the Site is in Failsoft. This error is SET when the Site Controller is not operating. The condition does not affect audio and the Site is still capable of trunked operation. Patch and Simulselect are affected in some system configurations.	Minor
CI_Ctrlr_Bd_Conflict	Multiple Controller Boards have the same assignment (dip switch settings).	**Major**
CI_No_Poll_Response	Controller Board did not respond to MOM Controller poll. The Controller Board has been removed or possibly failed. **NOTE:** This event does not affect icon color.	**Major**
CI_FE_Violation	Feature Encryption Violation. Capacity has been exceeded (using equipment not licensed, e.g., more consoles than have licenses for) or license has expired. **NOTE:** This event does not affect icon color.	**Major**
CI_FE_Warning	Feature Encryption Warning. License is about to expire. **NOTE:** This event does not affect icon color.	Warning

9.1.2 CEC/IMC PC Alarms

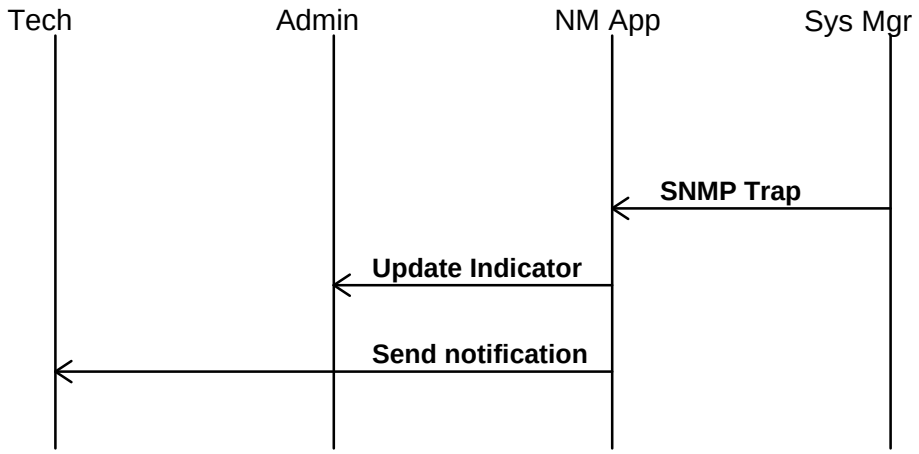
Alarm SET/RESET Use Case



FAULT NAME	DESCRIPTION	SEVERITY LEVEL
IM_MomCtrl_Link_Fail	CEC/IMC Manager PC-to-MOM Controller Link Failure.	**Major**
coldStart	A coldStart trap signifies that the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.	Normal
linkDown	A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.	Minor
linkUp	A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.	Normal
authenticationFailure	An authenticationFailure trap signifies that the sending protocol entity is the addressee of a protocol message that is not properly authenticated. While implementations of the SNMP must be capable of generating this trap, they must also be capable of suppressing the emission of such traps via an implementation-specific mechanism.	Warning

9.1.3 System Manager Alarms

Alarm SET/RESET Use Case

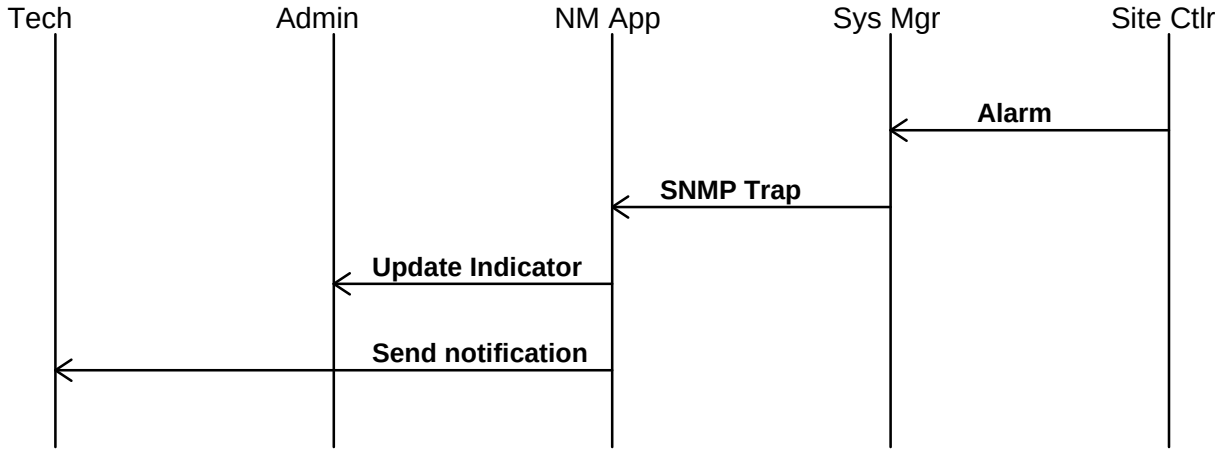


FAULT NAME	DESCRIPTION	SEVERITY LEVEL
SM_Disk_Warning	An indication that system disk free space has fallen below 10,000 blocks.	Warning
SM_Disk_Critical	An indication that the system disk has less than 5000 free blocks and performance may be severely degraded.	Warning
SM_DiskMgrWarningSet	An indication that the Disk Space Manager has detected that free space has fallen below the warning threshold set in screen 77 of the System Manager.	Warning
SM_DiskMgrDeletion	An indication that the Disk Space Manager has detected that free space has fallen below the Deletion Threshold set in screen 77 of the System Manager.	Minor
SM_DiskMgrWarningClr	An indication that the Disk Space Manager has detected that free space has once again increased above the warning threshold as set in screen 77 of the System Manager.	Warning
SM_IMC_Link_Change	An indication that a serious failure has occurred regarding the System Manager-to-IMC communication link. Fault can be at the System Manager, Site Controller, or the link itself.	**Major**
SM_Site_Link_Change	An indication that a serious failure has occurred regarding the System Manager-to-Site Controller communication link. Fault can be at the System Manager, Site Controller, or the link itself.	**Major**
SM_AppSW_Integrity	An indication that a serious unrecoverable problem has occurred relating to the EDACS Network Manager interface on the System Manager, and a reboot may be required.	**Major**

coldStart	A coldStart trap signifies that the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.	Normal
linkDown	A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.	Minor
linkUp	A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.	Normal
authenticationFailure	An authenticationFailure trap signifies that the sending protocol entity is the addressee of a protocol message that is not properly authenticated. While implementations of the SNMP must be capable of generating this trap, they must also be capable of suppressing the emission of such traps via an implementation-specific mechanism.	Warning

9.1.4 Site Controller Alarms

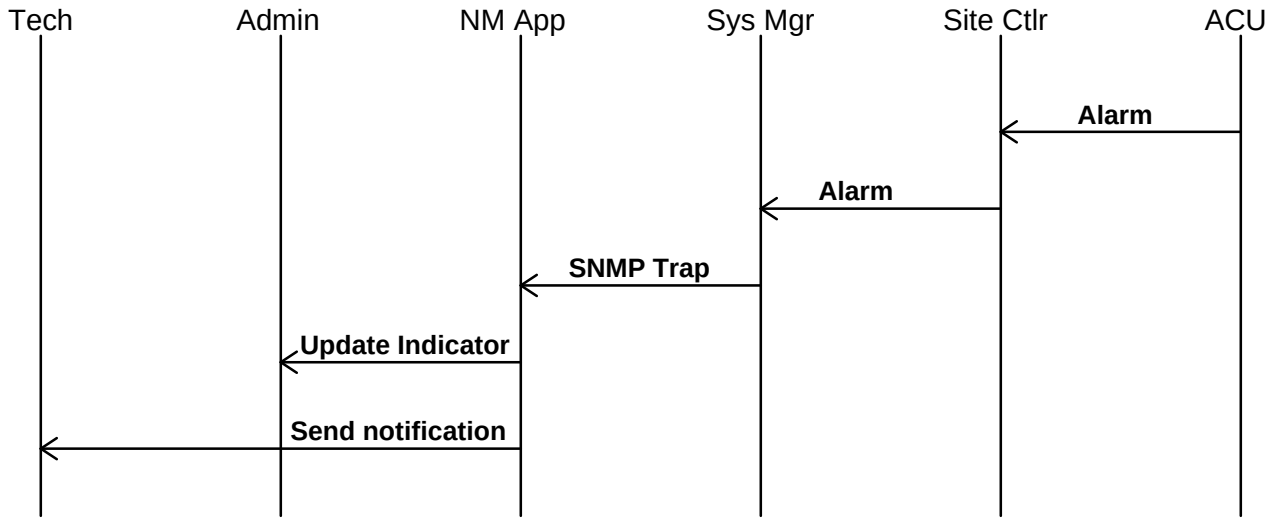
Alarm SET/RESET Use Case



FAULT NAME	DESCRIPTION	SEVERITY LEVEL
SC_GETC_Poll_Fail	This alarm is generated when a GETC fails to respond to Site Controller polling. The Site Controller assumes that the GETC is defective and does not assign it for use as a Control or Working Channel until it begins to respond to poll messages again.	Minor
SC_RIC_Poll_Fail	This alarm is generated when a Repeater Interconnect Controller (RIC) fails to respond to Site Controller polling.	Minor
SC_ACU_Poll_Fail	The Site Controller generates this alarm if the Alarm and Control Unit (ACU) does not respond to poll messages. The Site Controller will always issue this alarm if the ACU is not installed.	Minor
SC_LIC_Poll_Fail	The Site Controller generates this alarm if the Line Interconnect Controller (LIC) does not respond to poll messages. The Site Controller will always issue this alarm if the LIC is not installed.	Minor
SC_PMU_Poll_Fail	The Site Controller will always generate this alarm if the Power Monitor Unit (PMU) does not respond to poll messages or if the PMU is not installed. The Site Controller will also generate this alarm if the System Manager issues a disable command (user generated) or if the number of failed channels exceeds a preset limit.	Minor
SC_TU_Poll_Fail	The Site Controller will always generate this alarm if the Test Unit (TU) does not respond to poll messages or if the TU is not installed. The Site Controller will also generate this alarm if the System Manager issues a disable command (user generated) or if the number of failed channels exceeds a preset limit.	Minor

9.1.5 Alarm Control Unit (ACU) Alarms

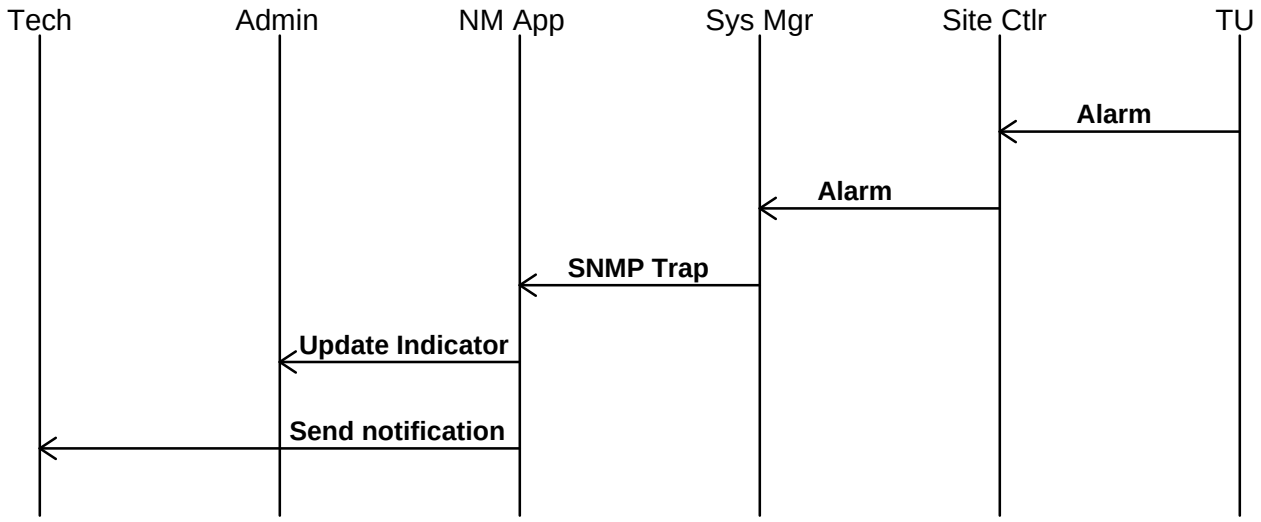
Alarm SET/RESET Use Case



FAULT NAME	DESCRIPTION	SEVERITY LEVEL
ACU_Lead_Change	An indication that one of the Alarm Control Unit's (ACU's) 32 alarm leads has been activated. These leads are defined using the ACU definition screen (screen 16) within the System Manager.	Warning

9.1.6 Test Unit (TU) Alarms

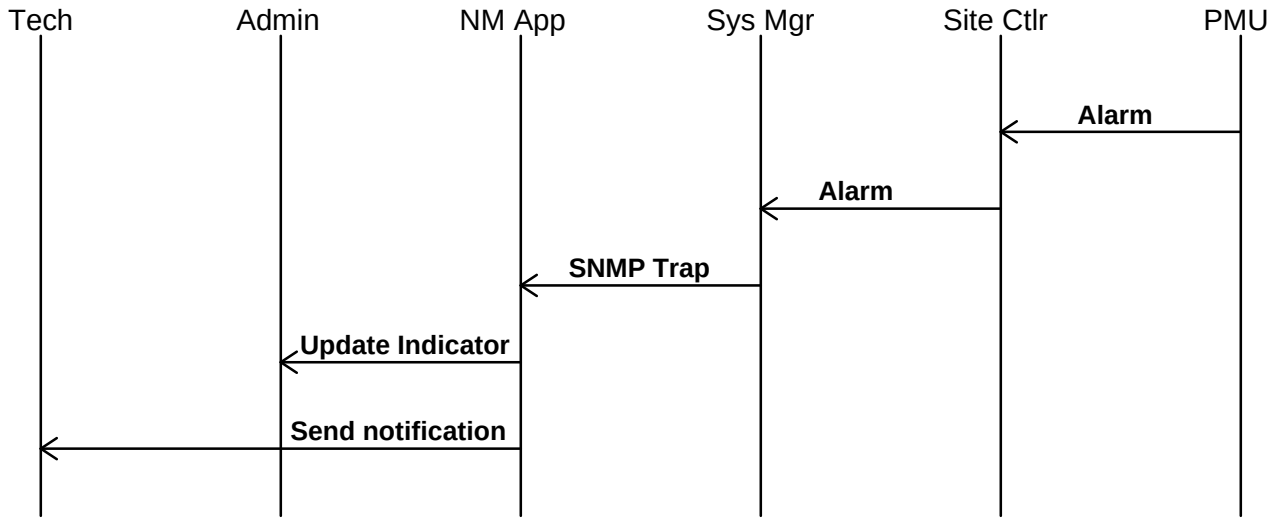
Alarm SET/RESET Use Case



FAULT NAME	DESCRIPTION	SEVERITY LEVEL
TU_GETC_Channel_Fail	This alarm is generated when the Test Unit (TU) detects a failure during RF testing of a Working Channel or if the high-speed data transmission from the Control Channel is interrupted.	Minor

9.1.7 Power Monitor Unit (PMU) Alarms

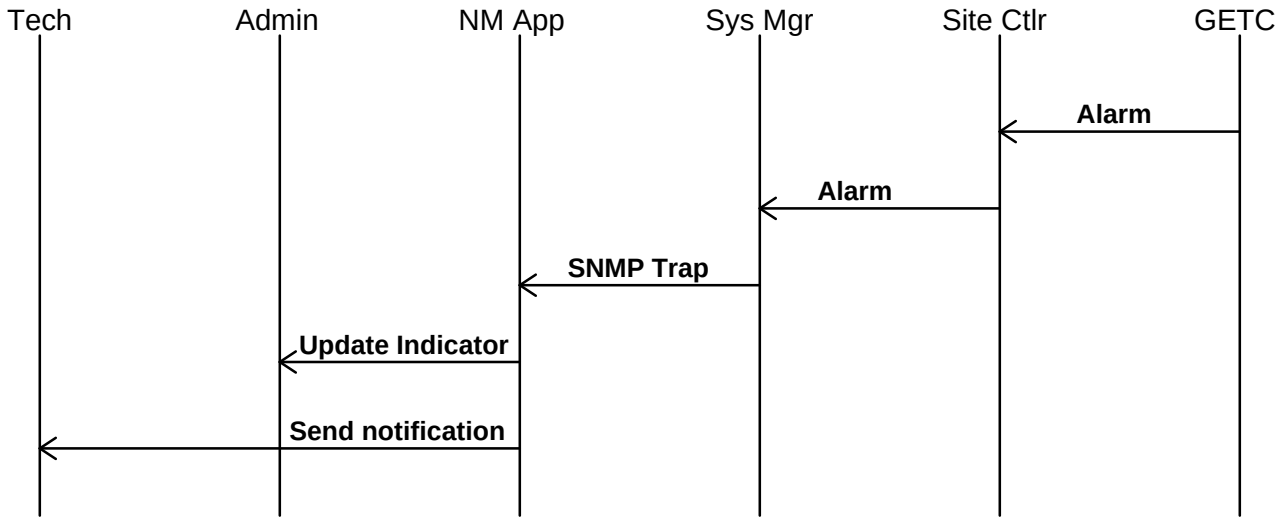
Alarm SET/RESET Use Case



FAULT NAME	DESCRIPTION	SEVERITY LEVEL
PMU_Channel_RF_Power	This alarm is issued when the transmitter's output power drops below the Power Monitor Unit (PMU) power level set within the System Manager (screen 3:4, menu item 10). The PMU sends an alarm status message to the Site Controller, which takes the channel out of service.	Minor
PMU_Antenna_Feed	This alarm is issued when the Power Monitor Unit (PMU) determines that the antenna voltage standing wave ratio (VSWR), which is calculated from the power sensor's forward and reverse power measurements, has exceeded the threshold values programmed into the PMU.	**Major**

9.1.8 GETC Alarms

Alarm SET/RESET Use Case

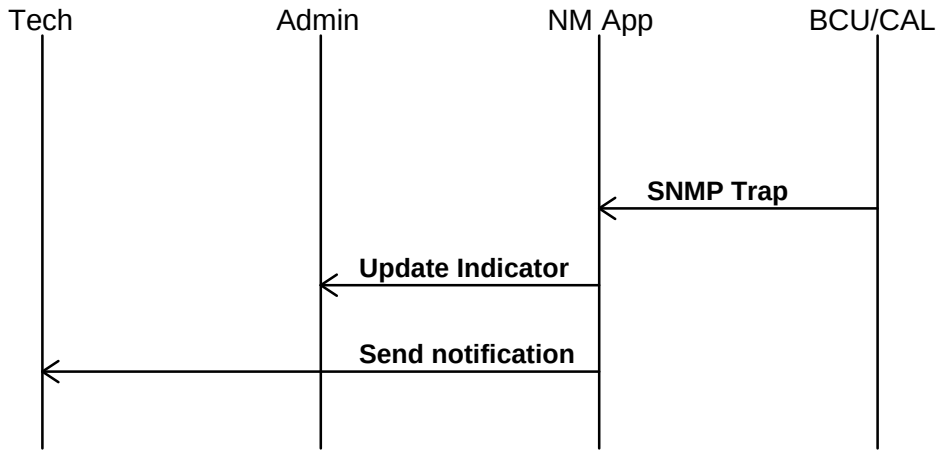


FAULT NAME	DESCRIPTION	SEVERITY LEVEL
GETC_Carrier_Change	Each station GETC (Control Channel or Working Channel) monitors its RF carrier for proper high-speed EDACS signaling. If an RF carrier is present without proper signaling then an alarm condition exists. This may be caused by an interfering signal or a deliberate jamming effort. The GETC notifies the Site Controller of the unexpected carrier and the Site Controller reassigns the Control Channel to another GETC or stops assigning the GETC as a working channel until the problem clears.	Warning
GETC_Phone_Line	Phone Line is a name given to the GETC's Rockwell Modem 9600-baud synchronous serial port. Any loss of data will be detected and will generate this failure. This failure may be caused by line noise or breakage.	Minor
GETC_AUX_Change	This alarm is generated when the remote test unit notifies the Site Controller via the System Alarm and Control Point GETC that a channel has failed. This alarm is typically used only with Simulcast systems. Each station GETC monitors the Simulcast Alarm System for a fault condition through a control line. The Auxiliary Alarm System will change the state of this line, creating an alarm condition. This may be the result of a failed test call, receiver fault, loss of low-speed data, etc.	Minor

FAULT NAME	DESCRIPTION	SEVERITY LEVEL
GETC_FSL_Internal	This alarm is generated when the GETC detects an internal error relating to Frame Sync Link (FSL) functionality. The FSL is a single wire connecting all site GETCs, allowing high-speed data synchronizing. The slave devices monitor this line and detect a pulse width absence or abnormality as a failure. This may be caused by a line open/short or a fault in the Control Channel which drives the line.	Minor
GETC_Power_Fail	Each station GETC monitors its RF power level through a control line driven by the station or power sensor. If the power level drops below a threshold level, an alarm condition exists. This may be caused by a PA failure, antenna failure, or high line voltage standing wave ratio (VSWR).	Minor
GETC_Synthesizer	Each station GETC monitors the frequency synthesizer for locked condition through a control line. If the GETC fails to detect a synthesizer locked condition, then an alarm condition exists. This may be caused by a faulty synthesizer or failure of the GETC to load the synthesizer.	Minor
GETC_Turbo_Fail	The main GETC processor and Turbo communicate through a specialized RAM interface. If communication is disrupted, then an alarm condition exists. This may be caused by a turbo failure, incorrect software version, or turbo turned off.	Minor
GETC_Voter_Failure	The GETC monitors the phone port (Rockwell Modem) for error messages from the Voter. If the Voter error messages are received, then an alarm condition exists. This is a summary alarm and may be caused by any number of Voter failures.	Minor

9.1.9 BCU/CAL Alarms

Alarm SET/RESET Use Case

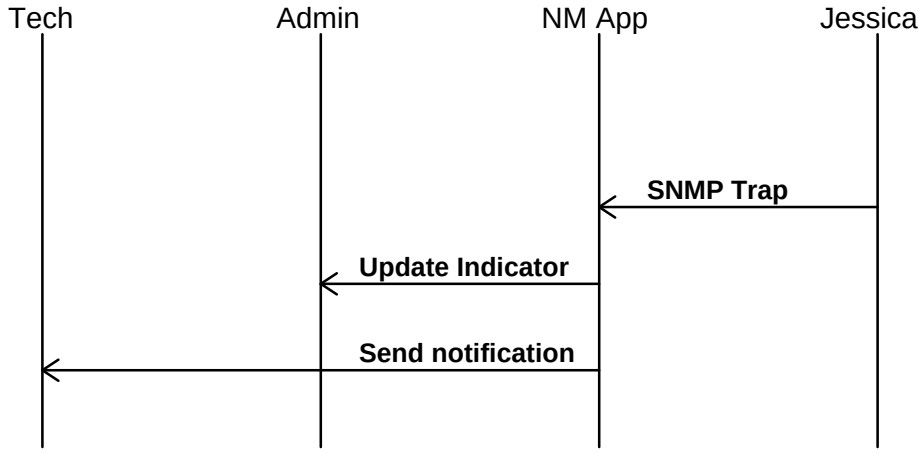


FAULT NAME	DESCRIPTION	SEVERITY LEVEL
BC_Falling_Thrld	An alarm entry has crossed its falling threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.	Warning
BC_Rising_Thrld	An alarm entry has crossed its rising threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.	Warning
BC_Remote_Reset	An indication that the sending entity is in the process of performing a complete system reset. The operRemoteReset object instance contains the current state of the reset process, which will (typically) be either inProgress(3) or finalNotice(4).	Normal
BC_Status_Update	An indication that the sending entity has detected a significant change in it's operational status. The Remote Status contains the current operational state.	Normal
coldStart	A coldStart trap signifies that the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.	Normal
linkDown	A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.	Minor
linkUp	A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.	Normal

authenticationFailure	An authenticationFailure trap signifies that the sending protocol entity is the addressee of a protocol message that is not properly authenticated. While implementations of the SNMP must be capable of generating this trap, they must also be capable of suppressing the emission of such traps via an implementation-specific mechanism.	Warning

9.1.10 Jessica PI Alarms

Alarm SET/RESET Use Case



FAULT NAME	DESCRIPTION	SEVERITY LEVEL
PI_WAN_Board_Change	An indication that the sending entity has detected a significant change in the status of the WANServer board.	**Major**
PI_DS1_Board_Change	An indication that the sending entity has detected a significant change in the status of a PRI board.	**Major**
PI_Ctrl_Link_Change	An indication that the sending entity has detected a significant change in the status of a PI-IMC control link.	**Major**
PI_PBX_Link_Change	An indication that the sending entity has detected a significant change in the status of a LAPD (PI to MD110) control link.	**Major**
PI_DS1_Trunk_Status	An indication that the sending entity has detected a significant change in a DS1 trunk's operational status.	**Major**
PI_Falling_Thrld	An alarm entry has crossed its falling threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.	Warning
PI_Rising_Thrld	An alarm entry has crossed its rising threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.	Warning
PI_Remote_Reset	An indication that the sending entity is in the process of performing a complete system reset. The operRemoteReset object instance contains the current state of the reset process, which will (typically) be either inProgress(3) or finalNotice(4).	Normal
PI_Status_Update	An indication that the sending entity has detected a significant change in it's operational status. The Remote Status contains the current operational state.	Normal

coldStart	A coldStart trap signifies that the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.	Normal
linkDown	A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.	Minor
linkUp	A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.	Normal
authenticationFailure	An authenticationFailure trap signifies that the sending protocol entity is the addressee of a protocol message that is not properly authenticated. While implementations of the SNMP must be capable of generating this trap, they must also be capable of suppressing the emission of such traps via an implementation-specific mechanism.	Warning

9.2 CONFIGURATION MANAGEMENT

In general, Configuration Management is via native access via Telnet into the System Manager, BCU/CAL, and PI. Our strategy is to migrate the implementation of the remote configuration platforms to the client-server paradigm. The CEC/IMC Manager for Windows NT is implemented this way. This allows the CEC/IMC Manager user interface to be run either on the EDACS Network Manager or on the CEC/IMC Manager PC.

9.3 ACCOUNTING MANAGEMENT

Accounting Management is responsible for capturing the usage of network resources by end users and the generation of billing information.

Billing subsystems are available on the BCU (stand-alone), the 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.

9.4 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.

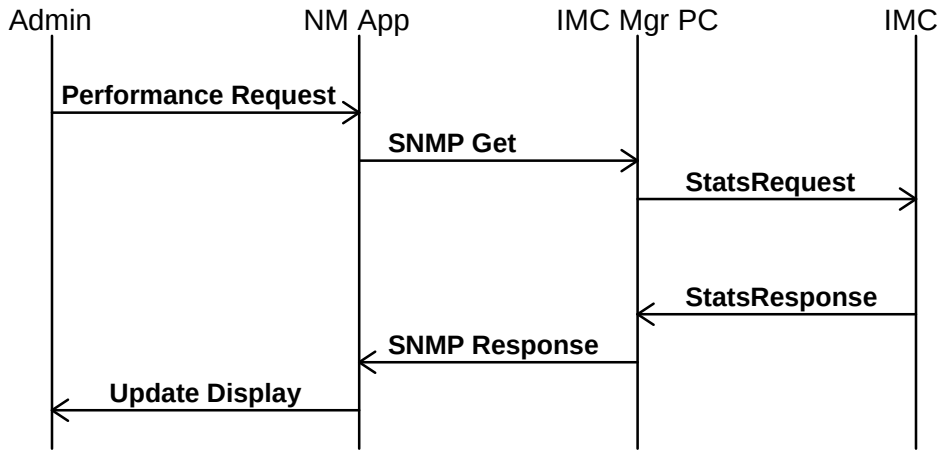
All managed EDACS devices provide various performance values via predefined SNMP Management Information Bases (MIBs). The EDACS NM requests and receives these values for display and/or collection. The performance values required, and the network element(s) responsible for providing them, are given in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

Graphs to address Utilization and Accessibility may be invoked via menu items.

EDACS SNMP Agents can restrict management station access to MIB objects to read only or read/write by specifying the access level for each IP address.

9.4.1 CEC/IMC Performance

Performance Request Use Case

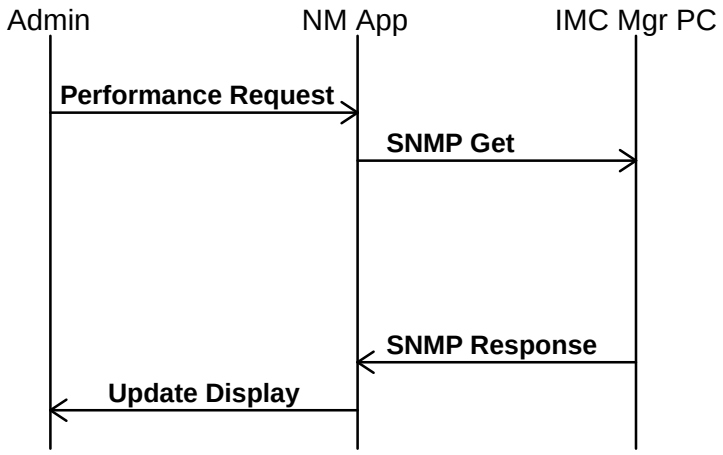


GSC STATISTICS	
PERFORMANCE PARAMETER	**APPLICABLE CONTROLLER BOARD TYPE**
GSC transmit errors	All
GSC receive errors	All
GSC percent loading	All
Missed channel assignments	MIM, VMIM, CTIM, DVIM, PIM, NIM
Missed channel drops	MIM, VMIM, CTIM, DVIM, PIM, NIM
152-to-186 dual port buffer serial msg overflows	All
152-to-186 dual port buffer GSC msg overflows	All
152-to-186 dual port buffer internal msg overflows	All
186-to-152 dual port buffer serial msg overflows	All
186-to-152 dual port buffer GSC msg overflows	All
186-to-152 dual port buffer internal msg overflows	All

NIM STATISTICS	
PERFORMANCE PARAMETER	**APPLICABLE CONTROLLER BOARD TYPE**
Channel Assignments	NIM
Calls queued	NIM
Calls blocked	NIM
Avg queue depth	NIM
Queue time-outs	NIM
Early unkeys	NIM
Link failures	NIM
Link state	NIM
Avg queue time	NIM
Call status	NIM
Queue status	NIM

9.4.2 CEC/IMC Manager Performance

Performance Request Use Case



ISO organizes parameters believed to be generic across all devices supporting SNMP into a specification called MIB-II. MIB-II has parameters used in fault, configuration, accounting, and performance status. MIB-II is composed of several SNMP groups. The groups which may have been implemented and which may have performance characteristics of interest are listed in the table below.

GROUP NAME	STARTING NODE	COMMENTS
system	1.3.6.1.2.1.1	Mandatory - Fully implemented (NT).
interfaces	1.3.6.1.2.1.2	Mandatory - Fully implemented (NT).
at	1.3.6.1.2.1.3	Not implemented.
ip	1.3.6.1.2.1.4	Implemented - NT v3.50 agent.
icmp	1.3.6.1.2.1.5	Implemented - NT v3.50 agent.
tcp	1.3.6.1.2.1.6	Implemented - NT v3.50 agent.
udp	1.3.6.1.2.1.7	Implemented - NT v3.50 agent.
egp	1.3.6.1.2.1.8	Not implemented.
transmission	1.3.6.1.2.1.10	Not implemented
snmp	1.3.6.1.2.1.11	Not implemented.

NOTE: This partially implements common parameters.

HDLC STATISTICS	
PERFORMANCE PARAMETER	**APPLICABLE HDLC CHANNELS**
.I Frames Queued	A,B
.I Frames Transmit	A,B
.I Frames Received	A,B
.I Frames Discarded	A,B
.I Frame Queue Ovfl	A,B
.S Frames Queued	A,B
.S Frames Transmit	A,B
.S Frames Received	A,B
.S Frames Discarded	A,B
.S Frame Queue Ovfl	A,B
.U Frames Queued	A,B
.U Frames Transmit	A,B
.U Frames Received	A,B
.U Frames Discarded	A,B
.U Frame Queue Ovfl	A,B
.Tx errors	A,B
.Rx errors	A,B
.U FRMR queued	A,B
.U FRMR received	A,B
.T1 polls	A,B
.Rx queue overflow	A,B
.Audio board active	A,B

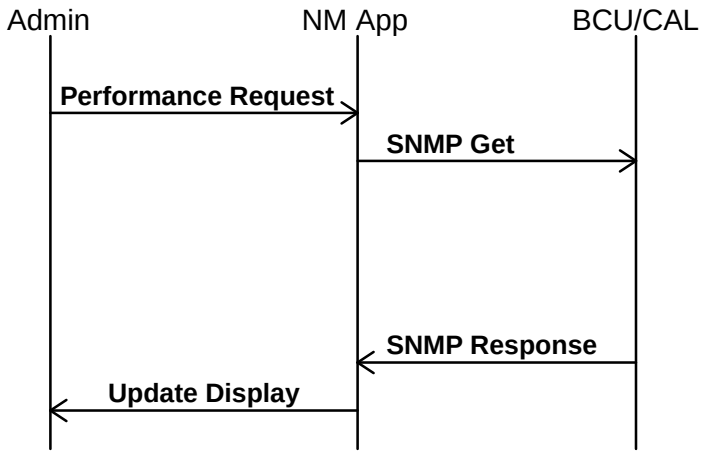
9.4.3 Node Performance

NOTE

In order to obtain node performance, a BCU/CAL or Jessica must be present in the system.

The majority of these parameters may be invoked via menu items.

Performance Request Use Case



UTILIZATION
Total RF time for all call types
Individual Voice Call total RF time
Group Voice Call total RF time
Individual Data Call total RF time
Group Data Call total RF time
Individual Outbound Interconnect Call total RF time
Individual Inbound Interconnect Call total RF time
Group Inbound Interconnect Call total RF time
Other Call total RF time

QUEUING DURATION
Total queuing time for all call types
Individual Voice Call total queuing time
Group Voice Call total queuing time
Individual Data Call total queuing time
Group Data Call total queuing time
Individual Outbound Interconnect Call total queuing time
Individual Inbound Interconnect Call total queuing time
Group Inbound Interconnect Call total queuing time
Other Call total queuing time

CHANNEL ASSIGNMENT
Total channel assignments for all call types
Total channel assignments for emergency calls
Total channel assignments for multisite calls
Total channel assignments for message trunked calls
Total drops for all call types
Individual Voice Call total channel assignments
Group Voice Call total channel assignments
Individual Data Call total channel assignments
Group Data Call total channel assignments
Individual Outbound Interconnect Call total channel assignments
Individual Inbound Interconnect Call total channel assignments
Group Inbound Interconnect Call total channel assignments
Other Call total channel assignments

QUEUE TOTALS
Total queued for all call types
Individual Voice Call total queued
Group Voice Call total queued
Individual Data Call total queued
Group Data Call total queued
Individual Outbound Interconnect Call total queued
Individual Inbound Interconnect Call total queued
Group Inbound Interconnect Call total queued
Other Call total queued

DENY TOTALS
Total denies for all call types
Individual Voice Call total denies
Group Voice Call total denies
Individual Data Call total denies
Group Data Call total denies
Individual Outbound Interconnect Call total denies
Individual Inbound Interconnect Call total denies
Group Inbound Interconnect Call total denies
Other Call total denies

BUSY TOTALS
Total system busies for all call types
Individual Voice Call total system busies
Group Voice Call total system busies
Individual Data Call total system busies
Group Data Call total system busies
Individual Outbound Interconnect Call total system busies
Individual Inbound Interconnect Call total system busies
Group Inbound Interconnect Call total system busies
Other Call total system busies

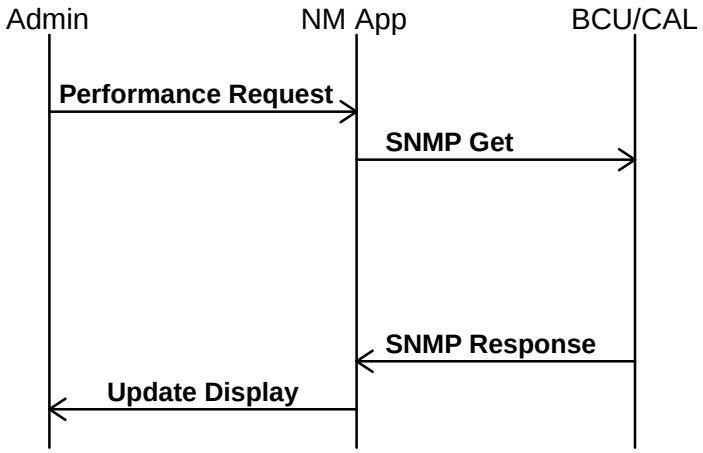
9.4.4 Site Performance

NOTE

In order to obtain node performance, a BCU/CAL or PI must be present in the system.

The majority of these parameters may be invoked via menu items.

Performance Request Use Case



UTILIZATION
Total RF time for all call types
Individual Voice Call total RF time
Group Voice Call total RF time
Individual Data Call total RF time
Group Data Call total RF time
Individual Outbound Interconnect Call total RF time
Individual Inbound Interconnect Call total RF time
Group Inbound Interconnect Call total RF time
Other Call total RF time

QUEUING DURATION
Total queuing time for all call types
Individual Voice Call total queuing time
Group Voice Call total queuing time
Individual Data Call total queuing time
Group Data Call total queuing time
Individual Outbound Interconnect Call total queuing time
Individual Inbound Interconnect Call total queuing time
Group Inbound Interconnect Call total queuing time
Other Call total queuing time

CHANNEL ASSIGNMENT
Total channel assignments for all call types
Total channel assignments for emergency calls
Total channel assignments for multisite calls
Total channel assignments for message trunked calls
Total drops for all call types
Total channel keys
Total channel unkeys
Individual Voice Call total channel assignments
Group Voice Call total channel assignments
Individual Data Call total channel assignments
Group Data Call total channel assignments
Individual Outbound Interconnect Call total channel assignments
Individual Inbound Interconnect Call total channel assignments
Group Inbound Interconnect Call total channel assignments
Total converted caller to callee
Other Call total channel assignments

QUEUE TOTALS
Total queued for all call types
Individual Voice Call total queued
Group Voice Call total queued
Individual Data Call total queued
Group Data Call total queued
Individual Outbound Interconnect Call total queued
Individual Inbound Interconnect Call total queued
Group Inbound Interconnect Call total queued
Other Call total queued

DENY TOTALS
Total denies for all call types
Individual Voice Call total denies
Group Voice Call total denies
Individual Data Call total denies
Group Data Call total denies
Individual Outbound Interconnect Call total denies
Individual Inbound Interconnect Call total denies
Group Inbound Interconnect Call total denies
Other Call total denies

BUSY TOTALS
Total system busies for all call types
Individual Voice Call total system busies
Group Voice Call total system busies
Individual Data Call total system busies
Group Data Call total system busies
Individual Outbound Interconnect Call total system busies
Individual Inbound Interconnect Call total system busies
Group Inbound Interconnect Call total system busies
Other Call total system busies

9.4.5 System Manager Performance

ISO organizes parameters believed to be generic across all devices supporting SNMP into a specification called MIB-II. MIB-II has parameters used in fault, configuration, accounting, and performance status. MIB-II is composed of several SNMP groups. The groups which may have been implemented and which may have performance characteristics of interest are listed in the table below.

MIB-II as specified in the table below if available from TGV Agent.

GROUP NAME	STARTING NODE	COMMENTS
system	1.3.6.1.2.1.1	Provided by TGV Agent.
interfaces	1.3.6.1.2.1.2	Provided by TGV Agent.
at	1.3.6.1.2.1.3	Not implemented.
ip	1.3.6.1.2.1.4	Provided by TGV Agent.
icmp	1.3.6.1.2.1.5	Provided by TGV Agent.
tcp	1.3.6.1.2.1.6	Provided by TGV Agent.
udp	1.3.6.1.2.1.7	Provided by TGV Agent.
egp	1.3.6.1.2.1.8	Not implemented.
transmission	1.3.6.1.2.1.10	Not implemented
snmp	1.3.6.1.2.1.11	Provided by TGV Agent.

NOTE: This partially implements common parameters.

9.4.6 Site Controller Performance

Site performance parameters are presented in the Site Performance section above (9.4.4).

9.4.7 GETC Performance

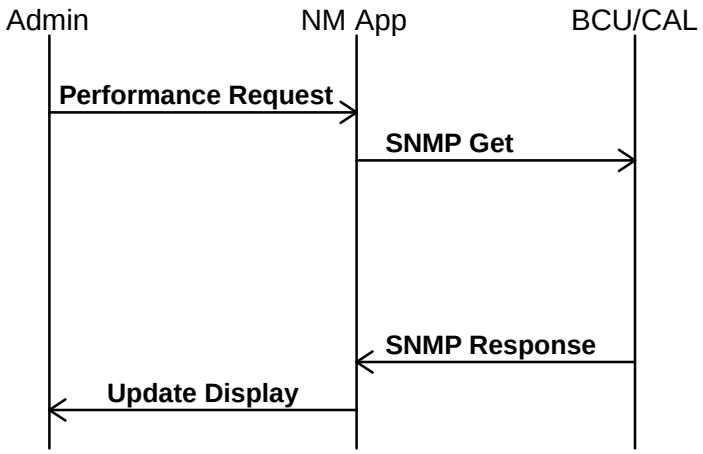
Site performance parameters are presented in the Site Performance section above (9.4.4).

9.4.8 Console Performance

No performance parameters have been identified for the Console.

9.4.9 BCU/CAL Performance

Performance Request Use Case



ISO organizes parameters believed to be generic across all devices supporting SNMP into a specification called MIB-II. MIB-II has parameters used in fault, configuration, accounting, and performance status. MIB-II is composed of several SNMP groups. The groups which may have been implemented and which may have performance characteristics of interest are listed in the table below.

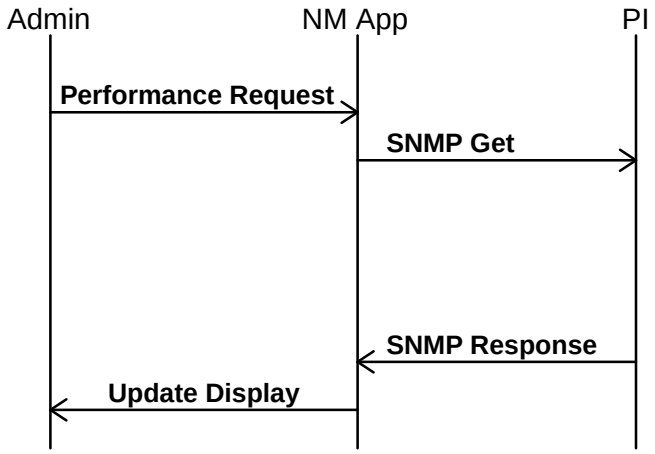
GROUP NAME	STARTING NODE	COMMENTS
system	1.3.6.1.2.1.1	Fully implemented.
interfaces	1.3.6.1.2.1.2	Fully implemented.
at	1.3.6.1.2.1.3	Not implemented.
ip	1.3.6.1.2.1.4	Fully implemented.
icmp	1.3.6.1.2.1.5	Fully implemented.
tcp	1.3.6.1.2.1.6	Fully implemented.
udp	1.3.6.1.2.1.7	Fully implemented.
egp	1.3.6.1.2.1.8	Not implemented.
transmission	1.3.6.1.2.1.10	RFC-1381: lapb - transmission(16). **Note(1)**
snmp	1.3.6.1.2.1.11	Fully implemented.

Note(1): RFC-1381 is the MIB for LAPB type interfaces. This MIB applies to the BCU-IMC control link(s). This MIB shall be partially implemented.

NOTE: This device implements site, node, and common parameters.

9.4.10 Jessica PI Performance

Performance Request Use Case



ISO organizes parameters believed to be generic across all devices supporting SNMP into a specification called MIB-II. MIB-II has parameters used in fault, configuration, accounting, and performance status. MIB-II is composed of several SNMP groups. The groups which may have been implemented and which may have performance characteristics of interest are listed in the table below.

GROUP NAME	STARTING NODE	COMMENTS
system	1.3.6.1.2.1.1	Fully implemented.
interfaces	1.3.6.1.2.1.2	Fully implemented.
at	1.3.6.1.2.1.3	Not implemented.
ip	1.3.6.1.2.1.4	Fully implemented.
icmp	1.3.6.1.2.1.5	Fully implemented.
tcp	1.3.6.1.2.1.6	Fully implemented.
udp	1.3.6.1.2.1.7	Fully implemented.
egp	1.3.6.1.2.1.8	Not implemented.
transmission	1.3.6.1.2.1.10	RFC-1406: ds1 - transmission(18). **Note(1)** RFC-1381: lapb - transmission(16). **Note(2)**
snmp	1.3.6.1.2.1.11	Fully implemented.

Note(1): RFC-1406 is the MIB for DS1 (T1/E1) type interfaces. This MIB applies to the T1/E1 trunk interfaces with the MD110 PBX, and IMC audio path(s). The Jessica PI partially implements the Near End Group Tables of RFC-1406.

Note(2): RFC-1381 is the MIB for LAPB type interfaces. This MIB applies to the PI-IMC call control link(s). This MIB shall be partially implemented for each LAPB interface between the PI and IMC.

This device implements site, node, and common parameters.

IMC INTERFACE STATISTICS
IMC Link Sampling Duration
Count of channel drops from IMC
Count of channel keys from IMC
Count of channel unkeys from IMC
Count of channel status messages from IMC
Count of phone digit messages from IMC
Count of Call Queued Messages from IMC
Count of System Busy messages from IMC
Count of Call Denied messages from IMC
Count of Channel assignments from IMC
Count of messages received from IMC with errors (discarded)
Count of SiteID messages sent to IMC
Count of Alerting messages sent to IMC
Count of System Busy messages sent to IMC
Count of Channel Confirmations sent to IMC
Count of Channel assignments sent to IMC
Count of Call Denied messages sent to IMC
Count of Channel Drops sent to IMC
Count of channel unkeys sent to IMC
Count of Interconnect CONNECT messages sent to IMC

INTERCONNECT CALL STATISTICS
Call Sampling Duration
Total number of calls
Total number of successful calls
Total number of inbound calls (phone to radio)
Total number of outbound calls (radio to phone)
Total number of calls from phone to radio, forwarded to another radio
Total number of calls from phone to radio, forwarded to another phone
Total number of calls from phone to radio, forwarded to a common phone
Total number of calls ended by normal disconnect
Total number of calls ended by callee busy disconnect
Total number of calls ended by no channel available disconnect
Total number of calls ended by an invalid id selected disconnect
Total number of calls ended by a time-out no answer disconnect
Total number of calls ended by a hang time expired disconnect
Total number of calls ended by a no phone digits disconnect
Total number of calls ended by a processing time-out disconnect
Total number of calls ended by a conversation limit exceeded disconnect
Total number of calls ended by a system busy disconnect
Total number of calls ended by a user denied disconnect
Total number of calls ended by a forced disconnect
Total number of calls ended by a failure disconnect
Total number of calls ended by a channel removed disconnect
Total number of calls ended by a do-not-disturb disconnect
Total number of calls ended by a forward error disconnect
Total number of calls ended by a feature success disconnect
Total number of calls ended by a feature fail disconnect
Total number of calls ended by a number restrict disconnect
Total number of calls ended by other disconnect causes

STATUS/FAULT PARAMETERS
Trunk Board Status .
PBX LABD Control Link status
Trunk Status (either PI-IMC or PI-MD110)
WAN Board Status
IMC Control Link Status
Count of Trunk Power Up Diagnostics Failures
Count of Trunk Run-Time Fatal Errors
Count of Trunk Run-Time Reboots
Count of PBX LAPD Link Downs
Count of WAN board Power Up Diagnostics Failures
Count of WAN board Run-Time Fatal Errors
Count of WAN board Run-Time Reboots
Count of IMC Control Link Downs

9.4.11 Common Managed Elements Parameters

MASS STORAGE PARAMETERS
Disk Component
Volume Name (i.e. file system component)
Volume Description (ascii text)
Media Type (hard disk, floppy disk, CD-ROM..)
Media Access (read only, read/write ...)
Media Removable
Block Size
Total Blocks
Free Blocks
Percent Blocks Used
Total File Descriptors (Inodes)
Total File Descriptors Free
Percent File Descriptors Used

REMOTE OPERATIONS PARAMETERS
Remote Reset/Reset Status
Reset Trap Enable
Remote Operational Status (shutdown, degraded, active..)
Operation Status Trap Enable
Date and Time

SOFTWARE CONFIGURATION PARAMETERS
EDACS System Object Identification (EDG, PI, etc.)
EDACS Node Number (associated IMC number)
EDACS Feature Code (place holder for feature encryption)
Software Component
Software Type (Operating System, application, etc.)
Software Media Kit Part Number
Software Major Revision
Software Minor Revision
Software Target Device (EDG, Site Controller, etc.)
Software Description (ascii text)
Software Additional Description (ascii text, i.e., exception release)
Software Status (unknown, running, not loaded)
Software Install Date

TRAP DESTINATIONS PARAMETERS
Number of Destinations enabled
Trap Address Component
IP Address

9.5 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.

9.5.1 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.

9.5.2 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.

10. GLOSSARY

TERM	DEFINITION
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 EDACS Administrator)	Administrators are those people responsible for centralized configuration of 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 are not encrypted. Aegis private mode also offers improved weak signal performance. In addition, since Aegis private transmissions are 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.

TERM	DEFINITION
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, 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.

TERM	DEFINITION
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.)**
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 receipt 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.

TERM	DEFINITION
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.
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.

TERM	DEFINITION
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.
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.

TERM	DEFINITION
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.
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.

TERM	DEFINITION
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.
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.

TERM	DEFINITION
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 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.

TERM	DEFINITION
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.
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

TERM	DEFINITION
	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 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.

TERM	DEFINITION
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.

11. INDEX

—U—

12. NETWORK MANAGER SURVEY

PROJECT INFORMATION

Sheet __ of ___

CUSTOMER/PROJECT: _____

CONTACTS:

	Customer System Administrator	Ericsson Inc. System Engineer
Name:	_____	_____
Phone:	_____	_____

LAN REQUIREMENTS

Please complete the form below for **each** Network Manager.

Does customer have an existing LAN and LAN support personnel? _____

Does customer have an existing LAN connecting IMC node locations? _____

Does customer intend to connect EDACS devices to his existing LAN? _____

COMMENTS

_____
_____
_____
_____
_____

PROJECT INFORMATION

Sheet ___ of ___

CUSTOMER/PROJECT: _____

USER ACCOUNTS[1]

This section addresses the user environment setup.

How many distinct user accounts do you desire? _____

List the pertinent data for each user account:

ACCOUNT NAME Enter name of specific account or user group.	**OPENVIEW ACCESS[2]** Indicate if Write version (W) or Read Only (RO).	**REDUCED MENU SET[3]** (Yes or No)	**ACCOUNT INFORMATION (Optional)** (May include account information such as Account's real name, office location, office phone, or home phone)
Support	**RO**	**No**	**Remote Support Account**

COMMENTS

_____
_____
_____
_____

[1] Refer to the Security Management section for suggested Access Levels.

[2] There is one write version of OpenView. You many either restrict the write version to one account (or group) or allow the first requester to get it. Refer to the LBI-39169 for the list of features available to the write version that are not available to the read version.

[3] You may simplify the user interface by reducing the menu items seen by individual user accounts. The menu items to be removed are the SNMP/MIB direct interface items and event configuration.

PROJECT INFORMATION

Sheet ___ of ___

CUSTOMER/PROJECT: _____

LOGIN ENVIRONMENT

An icon will be added to the VUE front panel which provides a friendly interface to invoke a read version of OpenView. The Network Manager Station can be configured to automatically bring down the OpenView and performance applications when the VUE front panel EXIT is selected. The downside is that all OpenView and performance applications will be brought down even if the user is logged in multiple times. Users with unique names will be unaffected. Without this option, if the applications are not manually exited before hitting the VUE EXIT, then the processes will be left running until manually killed.

Do you wish the VUE EXIT option be configured? _____

PRINTERS

The Network Manager can use a local printer or a network printer.

Do you have a local printer to connect? _____

What kind of printer is it? _____

Do you have a network printer to connect?_____

Is it existing or new? _____

IP Address: _____

Printer Host Name: _____

COMMENTS

_____
_____
_____
_____
_____

PROJECT INFORMATION

Sheet __ of ___

CUSTOMER/PROJECT: _____

NETWORK MANAGER

Please complete the form below for **each** Network Manager.

NM Host Name: _____ NM IP Address (in the form 000.000.00.000) _____

Subnet Mask (same for all devices) _____

Enter Network Manager information, if available:

For example:	Location:	Top Downtown Building	Location:	_____
	Contact:	George Bailey	Contact:	_____
	Phone:	(123) 456 7890	Phone:	_____
		_____	Other:	_____

Shall periodic fault status polling be performed (Note this will use minimal LAN bandwidth)? _____

If so, please enter the rate between physical device polls (value > 2 sec.) (recommend 10 min.). _____

Do you desire the Network Manager to synchronize it's clock to the IMC Manager? _____

If so, to which IMC node shall the clock be synchronized? _____

What is the rate of synchronization? (value > 1 min.) _____

Do you wish to group IMCs into separate regions? _____

If so, list the Region Names and designate (√) the nodes belonging in each region:

REGION NAME	NODE NUMBER																	
	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50

REGION NAME	NODE NUMBER																	
	51	52	53	54	55	56	57	58	59	60	61	62	63	64				

PROJECT INFORMATION

Sheet ___ of ___

CUSTOMER/PROJECT: _____

REMOTE X-STATIONS

Please complete the form below for **each** remote X-Station. For IP addresses use the form 000.000.00.000 or enter N/A.

HOST NAME:	IP ADDRESS	COMMENTS, LOCATION, or OWNER

COMMENTS

_____
_____
_____
_____
_____

PROJECT INFORMATION

Sheet ___ of ___

CUSTOMER/PROJECT: _____

EDACS CEC/IMC/RCEC NODE

Please complete this form for **each** CEC, IMC, or RCEC node.

NODE TYPE (check one): CEC:____(1 site max.) IMC:____ (1 to 32 sites) RCEC:____ (No sites)

EDACS NODE NUMBER: _____(33 to 64) EDACS NODE NAME: _____

NOTE: The EDACS Node Number is the number associated with the radio switch (CEC, IMC, Remote CEC).

NIM NUMBER: _____(1 to 32)

Enter IMC description if desired:

For example: Location: Top Downtown Building _____

Contact: George Bailey _____

Phone: (123) 456 7890 _____

Other: _____

DEVICE	IP ADDRESS (In the form 000.000.00.000)	HOST NAME:	COMMENTS
CEC/IMC/RCEC Manager:			
Jessica PI: PI Site Number:_____			
BCU/CAL:			
EDG: Sub-node #:_____ (1-32)			
System Manager:			

Place a check (below) for each console present:

Console 1 _____	Console 9 _____	Console 17 _____	Console 25 _____
Console 2 _____	Console 10 _____	Console 18 _____	Console 26 _____
Console 3 _____	Console 11 _____	Console 19 _____	Console 27 _____
Console 4 _____	Console 12 _____	Console 20 _____	Console 28 _____
Console 5 _____	Console 13 _____	Console 21 _____	Console 29 _____
Console 6 _____	Console 14 _____	Console 22 _____	Console 30 _____
Console 7 _____	Console 15 _____	Console 23 _____	Console 31 _____
Console 8 _____	Console 16 _____	Console 24 _____	Console 32 _____

COMMENTS

_____

_____

PROJECT INFORMATION

Sheet ___ of ___

CUSTOMER/PROJECT: _____

STARGATE NODE

Please complete this form for **each** StarGate node.

NOTE: The EDACS Node Number is the number associated with the radio switch (CEC, Remote CEC, IMC, or StarGate). For IP addresses use the form 000.000.00.000 or enter N/A.

EDACS NODE NUMBER: _____(33 to 64) EDACS NODE NAME: _____

Enter IMC description if desired:

For example: Location: Top Downtown Building _____

Contact: George Bailey _____

Phone: (123) 456 7890 _____

Other: _____ _____

_____ _____

DEVICE	IP ADDRESS (In the form 000.000.00.000)	HOST NAME:	COMMENTS
StarGate Manager:			

COMMENTS

_____
_____
_____
_____
_____
_____
_____
_____

PROJECT INFORMATION

Sheet ___ of ___

CUSTOMER/PROJECT: _____

EDACS SITE NUMBER

Please complete the form below for **each** site.

Site Name: _____

Node Number: _____ (33 to 64)

Site Number: _____ (1 to 32)

Which of the following peripherals are present are the site?

ACU	_____	PMU	_____	TU	_____
ELI	_____	Site Controller	_____	SIM:	_____

Is there a Site description:

For example:

Location:	Top Downtown Building	_____
Contact:	George Bailey	_____
Phone:	(123) 456 7890	_____
Other:	_____	_____
	_____	_____

Channel 1	_____	Channel 13	_____
Channel 2	_____	Channel 14	_____
Channel 3	_____	Channel 15	_____
Channel 4	_____	Channel 16	_____
Channel 5	_____	Channel 17	_____
Channel 6	_____	Channel 18	_____
Channel 7	_____	Channel 19	_____
Channel 8	_____	Channel 20	_____
Channel 9	_____	Channel 21	_____
Channel 10	_____	Channel 22	_____
Channel 11	_____	Channel 23	_____
Channel 12	_____	Channel 24	_____

COMMENTS

_____
_____
_____
_____
_____

Ericsson Inc.
Private Radio Systems
Mountain View Road
Lynchburg, Virginia 24502
1-800-592-7711 (Outside USA, 804-592-7711)

Printed in U.S.A.