

# CMS™ 400 LAN Internetworking Manager

## User's Guide

13D36A-7/D 11/96

**Milgo Solutions, Inc.**

1619 N. Harrison Parkway

P.O. Box 407044

Fort Lauderdale, FL 33340-7044

Internet: <http://www.milgo.com>



## Warranty

The period of warranty for this product starts on the date of sale to the original purchaser and extends 90 days for software and one year for hardware. Refer to Milgo Solutions, Inc. Limited Warranty for details.

Milgo Solutions requires a Return Material Authorization (RMA) prior to the return of any equipment under the provisions of the warranty. Please contact your authorized reseller or the nearest Milgo support center for details.

Third Edition, November, 1996

CMS is a trademark of Milgo Solutions, Inc. All other logos and product names are trademarks or registered trademarks of their respective companies.

©1999 Milgo Solutions, Inc.

All rights reserved. No part of this work covered by the copyright hereon may be reproduced or copied in any form or by any means — graphic, electronic, or mechanical, including photocopying, recording, taping, or information and retrieval systems — without written permission of the publisher. Any software furnished under a license may be used or copied only in accordance with the terms of such license.

Milgo Solutions, Inc. reserves the right to modify or revise all or part of this document without notice and shall not be responsible for any loss, cost, or damage, including consequential damage, caused by reliance on these materials.

Printed in U.S.A.

# Milgo Solutions

## Customer Information Contacts

---

### **CORPORATE HEADQUARTERS**

Milgo Solutions, Inc.  
1619 North Harrison Parkway  
Sunrise, Florida 33323-2802, U.S.A.  
Tel: (954)-846-1601/(800)-333-4143  
Fax: (954)-846-3935  
Internet: <http://www.milgo.com>

Call Milgo's Corporate Headquarters if you need the following information:

<b>Press</b>	<b>For:</b>
1	Billing or invoice information
2	Orders, product delivery or availability, and repairs
3	Sales
4	Field service
5	Training
6	Employee benefits and information
7	Corporate quality
8	Mailing or street addresses

For technical support, please contact your supplier/distributor with details of the issue.

### **MILGO SERVICE CONTRACT CUSTOMERS:**

For customers with Milgo Service Contracts or service requirements, contact the following offices:

#### **AMERICAS**

##### **U.S. and U.S. Multinational**

Milgo Solutions, Inc.  
1619 North Harrison Parkway  
Sunrise, Florida 33323-2802  
Tel: (954)-846-4569/(800)-366-0126  
Fax: (954)-846-1137

##### **EUROPE/MIDDLE EAST/AFRICA**

Milgo Solutions, Ltd  
Landata House, Station Road  
Hook, Hampshire, RG279JF, England  
Tel: +44 (0) 1256 763911  
Fax: +44 (0) 1256 764717

Milgo Solutions SA  
Parc du Colombier  
18 Rue Jules Saulnier  
93206 Saint-Denis  
Cedex, France  
Tel: +331 (0) 49 33 5800  
Fax: +331 (0) 49 33 5851

Milgo Solutions BV  
Poortweg 14  
2612 PA Delft  
The Netherlands  
Tel: +31 15 269 82 82  
Fax: +31 15 262 18 08

#### **ASIA/PACIFIC**

Contact your Milgo affiliate support center. (See next page for addresses and phone/fax numbers.)

### **MILGO AFFILIATE SUPPORT CENTERS:**

#### **AMERICAS Region**

Milgo Solutions, Inc.  
1619 North Harrison Parkway  
Sunrise, Florida 33323-2802, U.S.A.  
Tel: (954)-846-6116/(888)-722-2548  
Fax: (954)-846-3692  
email: [support@milgo.com](mailto:support@milgo.com)

#### **EUROPE/MIDDLE EAST/AFRICA Region**

Milgo Solutions, Ltd.  
Landata House, Station Road  
Hook, Hampshire, RG279JF, England  
Tel: +44 (0) 1256 761240  
Fax: +44 (0) 1256 382112  
email: [support.centre@milgo.com](mailto:support.centre@milgo.com)  
Internet: [www.milgo.com/emea](http://www.milgo.com/emea)  
Bulletin Board Service: +44 1256 766608 (PSTN)  
+44 1256 744832/3/4 (ISDN)

---

## **MILGO AFFILIATE SUPPORT CENTERS:**

### **ASIA/PACIFIC Region**

Milgo Solutions (Hong Kong), Ltd.  
Sun House 6th Floor  
181 Des Voeux Road, Central  
Hong Kong  
Tel: 852-2815-1886  
Fax: 852-2815-2895

Milgo Solutions (Hong Kong) supports:

- China (southern provinces)
- Japan
- Korea
- Hong Kong
- Macau
- Taiwan

Milgo Solutions (Singapore) Pte Ltd.  
26 Ayer Rajah Crescent, #04-06  
Ayer Rajah Industrial Estate  
Singapore 139944  
Tel: +65 779 2200  
Fax: +65 778 5400

Milgo Solutions (Singapore) supports:

- Brunei
- Indonesia
- Malaysia
- Philippines
- Singapore
- Thailand
- Australia
- New Zealand
- Rest of Indochina
  - Cambodia
  - Laos
  - Myanmar
  - Vietnam

Milgo Solutions (Beijing), Inc.  
Room 20659  
Beijing Friendship Hotel  
Beijing 100873  
Tel: 86-10-6849-8731  
Fax: 86-10-6849-8732

Milgo Solutions (Beijing) supports:

- China (northern provinces)

# About This Manual

---

## Manual Description

This manual is intended to help you understand and operate the CMS<sup>TM</sup> 400 LAN Internetworking Manager (LIM), an optional module of the CMS 400 Network Management System. This manual assumes that you are familiar with your network's configuration and the Intel-based personal computer you use to run CMS 400.

Refer to the following manuals for specifics about installing and using your CMS 400 System:

- *CMS 400 Installation Manual* (13D26A-14)
- *CMS 400 Reference Manual* (13D26A-10)
- *CMS 400 User's Guide* (13D26A-7)

This manual addresses specific operations of the CMS 400 LAN Internetworking Manager Module.

**Chapter 1 — Getting Started** provides an overview of the CMS 400 LAN Internetworking Manager Module (LIMM). It describes how CMS 400 communicates with the module. It also lists the network products managed by the CMS 400 LIM.

**Chapter 2 — SNMP Administration** covers LIMM SNMP administrative tasks. It includes procedures for setting up and managing the SNMP elements on the CMS 400 network.

**Chapter 3 — Configuring LAN Equipment** describes how to monitor SNMP MIBs, INX, and RNX devices

**Chapter 4 — Monitoring SNMP Devices** describes the equipment-monitoring functions of the LIMM.

**Chapter 5 — Control Operations** describes how to use LIM to control SNMP devices on the network.

**Appendix A — Network Interface Cards (NICs)** describes possible card types compatible with the CMS 400 Hub.

**Appendix B — Custom SNMP Applications: A Tutorial.** A step-by-step guide that creates a sample SNMP Application using the Define SNMP Application feature of LIMM.

## Terminology and Conventions

Text appearing on the computer screen is shown in System typeface:

RNX6500 Router Control

Characters you enter must be input exactly as shown in System bold type:

**RNX6500**

A key that must be pressed on the keyboard is shown within brackets:

[ENTER]

# Table of Contents

---

## Chapter 1 – Getting Started

About the CMS 400 LIM .....	1-1
Assumptions .....	1-1
Supplementary Manuals .....	1-2
Hardware Requirements .....	1-2
Software Requirements .....	1-2
LIM Features .....	1-3
TCP/IP and CMS 400 Setup .....	1-4
Configuring LIM .....	1-6
Discovering IP Devices .....	1-7
Using SNMP Community Names .....	1-8
Setting Up General SNMP Parameters .....	1-9
Setting Proxy Agent Parameters .....	1-10
Adding Devices to the Network Map .....	1-11

## Chapter 2 – SNMP Administration

Overview .....	2-1
Assumptions .....	2-1
SNMP Procedures .....	2-2
Viewing a MIB File .....	2-2
Viewing a Specific MIB Object .....	2-3
Adding a Foreign Device to the CMS 400 Database .....	2-3
Using Health Tables .....	2-5
Working With SNMP Traps .....	2-8
Creating User-Defined SNMP Applications .....	2-12

## Chapter 3 – Configuring LAN Equipment

Introduction .....	3-1
INX5000 Configuration .....	3-2
INX Managed 10 Base T Configuration .....	3-5
INX NTS Configuration .....	3-7
INX Token Ring CAU Configuration .....	3-12
INX 4000 Bridge Configuration .....	3-14
RNX6x00/6150 Bridge/Router Configuration .....	3-19
Configuring the RNX6300 Console .....	3-20

## Chapter 4 – Monitoring SNMP Devices

About This Chapter .....	4-1
Monitoring SNMP Devices .....	4-1

Monitoring INX5000 Devices.....	4-3
Examining the INX5000 Chassis.....	4-14
Examining the INX T-Ring CAU.....	4-16
Monitoring an RNX6x00/6150 Bridge/Router.....	4-16
Displaying RNX6x00/6150 Statistics.....	4-19

## **Chapter 5 – Control Operations**

About Control Operations.....	5-1
Reading/Writing SNMP MIB Variables.....	5-1
Opening and Rotating the INX5000 Chassis.....	5-2
Reinitializing an SNMP Device.....	5-3
Pinging an SNMP Device.....	5-3
Disabling and Enabling an SNMP Device.....	5-3
Rebooting an SNMP Device.....	5-4
Accessing Telnet from INX T-Ring CAU.....	5-4
Opening and Closing the RNX6x00 Panel.....	5-4
Accessing the Cut-Through to the RNX6300 Console.....	5-5
Directing SNMP GET/SET Control.....	5-5
Displaying MIB Objects in a Unit.....	5-5
Accessing Telnet from Generic SNMP Control.....	5-6
Accessing Telnet from an RNX6x00.....	5-6

## **Appendix A – Network Interface Card Types**

## **Appendix B – Custom SNMP Applications: A Tutorial**

# Chapter 1

## Getting Started

---

### About the CMS 400 LIM

The LAN Internetworking Manager (LIM) module of the CMS™ 400 lets you manage heterogeneous, multivendor networks, known as *internets*, from a CMS 400 workstation. The CMS 400 LIM lets you take advantage of the Simple Network Management Protocol (SNMP). SNMP is built on the Internet suite of protocols known as Transmission Control Protocol/Internet Protocol (TCP/IP).

Before you can run CMS 400's LIM option, you must physically connect the CMS 400 workstation to your Ethernet network via a network interface card (NIC). Also, on the CMS 400 hub, you need to install a TCP/IP application that supports SNMP. (Examples in this book refer to FTP Software's® PC/TCP® Network Software.)

---

**Note:** The LAN Internetworking Manager module is a separately purchased option for your CMS 400 System. Details for installing LIM and other CMS 400 options are provided in the *CMS 400 Installation Manual*.

---

If you have questions about hardware compatibility, TCP/IP compatibility, or LAN adapter cards, contact your Milgo Solutions sales representative.

This section covers the following topics:

- Assumptions about what you should already know
- Supplementary manuals
- CMS 400/LIM hardware requirements
- Software requirements
- LIM Features

### Assumptions

This manual assumes that you are familiar with the basics of personal computing, and with your network topology. Before setting up the LIM option, you should also understand:

- CMS 400 terminology such as: *hub*, *collapsed hub*, *EDM*, *DDM*, and *SDM*. (See the *CMS 400 Installation Manual*.)

- Basic concepts and terminology of Simple Network Management Protocol (SNMP) and Transmission Control Protocol/Internet Protocol (TCP/IP).

## Supplementary Manuals

In addition to this manual, refer to the following documentation when setting up the LAN Internetworking Manager module:

*CMS 400 Installation Manual*

*CMS 400 User's Guide*

The network interface card manual

The TCP/IP software manual(s)

## Hardware Requirements

To run LIM with CMS 400, you need an IBM-compatible (Intel 80x86) personal computer with the following *minimum* requirements:

- Intel 80486 processor
- 66 MHz clock speed, or faster
- 8 megabytes of memory
- Bus: ISA (EISA or 32-bit if SNMP traffic is heavy)
- NIC Card: ISA card or Etherblaster card (if EISA use an NI3210)
- Monochrome, CGA, EGA, or VGA video adapters (color preferred)
- Hard disk (if SNMP traffic is heavy, use a SCSI hard disk with 9.5 ms access time)
- Mouse/pointing device is recommended
- At least one serial (COM) port (not required for SNMP-only hub.)

## Software Requirements

The CMS 400 requires:

- DOS 5.0 or higher

The LAN Internetworking Manager option requires:

- A TCP/IP package that supports SNMP (examples in this book refer to FTP Software's<sup>®</sup> PC/TCP<sup>®</sup> Network Software)

If you have questions about hardware compatibility, TCP/IP compatibility, or LAN adapter cards, contact your Milgo Solutions sales representative.

## LIM Features

The LAN Internetworking Manager offers the following features:

- Built-in support (MIBs) for Milgo's RNX and INX line of gateway devices
- Network management for multivendor SNMP devices
- SNMP devices that can boot from the CMS 400 hub
- SNMP Top-16 MIB Monitor

### Milgo RNX/INX SNMP Support

The CMS 400 LIM allows you to configure, monitor, and manage Milgo's line of RNX and INX products. These SNMP devices are defined as unit types for the LIM. The following products are directly supported by LIM:

- INX5000 Chassis (3- and 12-slot), INX Link Chassis, and INX5000 modules:
  - INX-NTS terminal server
  - INX-10 Base T
  - 10-Base T concentrator
  - INX 10 Base 2
  - INX CAU
  - INX-CAU Token Ring CAU
  - INX-FOIRL fiber optic inter-repeater link
  - INX-CMM chassis management module
  - INX-NMM network management module
  - INX4000 local and remote bridges
- RNX6x00/6150 router series
- RNX6300 bridge
- InterLANLink stackable hub
- EAN 4000 and SR 4200

## **Multivendor SNMP Support**

The LAN Internetworking Manager's Generic SNMP Control lets you configure, monitor, and manage any SNMP device on your network. You can access Generic SNMP Control from LAN Control, Network Map, Big Picture, or Draw Network functions. You can also submit SNMP GET and SET requests from scripts or NetView.

## **SNMP Devices that Can Boot from the CMS 400**

Through LIM, SNMP devices can load their operating software across the LAN. The CMS 400 is enabled as Trivial File Transfer Protocol (TFTP) boot server, and the required device files are loaded onto the CMS 400 hub. Refer to the documentation for each SNMP device for specific information.

## **SNMP Top-16 MIB Monitor**

The LIM's SNMP Top-16 Monitor feature lets you poll up to 16 MIB variables. Information is displayed on a graph as data is received. You can monitor one MIB variable from up to 16 devices, 16 MIB variables from one device, or any combination thereof up to 16.

# **TCP/IP and CMS 400 Setup**

This section provides general information for configuring the network interface card (NIC) and the TCP/IP (SNMP) software on the CMS 400 hub. For specifics, refer to the vendors' manuals that came with your NIC and with your TCP/IP software.

Use the following sequence of steps as a guideline when installing your TCP/IP hardware and software:

### **Step 1: Configuring the Network Interface Card**

First, install the network interface card (NIC) in your PC as specified by the vendor's manual. Be sure to write down the current jumper settings, especially if you are using an NI5210 or NI6510 interface card.

If you're installing an NI9210 (Micro channel) or ES3210 (EISA) NIC, you need to run your system's automatic configuration utility. This allows you to set up the NIC after it has been installed. (IRQ levels of 3 and 9 should not be used.)

## Step 2: Installing TCP/IP software

Before you begin the TCP/IP installation, you will need specific information about your company's TCP/IP network. If you fill out the TCP/IP Installation Checklist below, you should be prepared to install TCP/IP. Check with your vendor's documentation for complete details, and contact your network administrator for network-specific information.

### TCP/IP Installation Checklist

Required Information	Your Entry
TCP/IP Serial Number	
TCP Authentication Key	
Name of NIC	
NIC Frame (Network Type)	
NIC Interrupt Vector (IRQ)	
NIC Input/Output Address	
NIC Base Memory Address	
IP Address of Workstation	
Subnet Mask	
IP Address(es) of Default Router	
Hostname of your PC	
Domain Name of Your Host	
IP Address(es) of DNS	

### Sample TCP/IP Installation

The following is a sample TCP/IP installation script based on PC/TCP software. For details, refer to your TCP/IP installation manual. When you begin installation, keep your TCP/IP Checklist handy.

Insert Installation Disk in drive A and type INSTALL.

**A:INSTALL**

Destination directory drive [and path]: **C:\PCTCP**

Which drive is the distribution disk in? **A**

Target directory does not exist - create? **YES**

Do you want copy all the programs? **YES**

Do you want to add other programs to the list? **NO**

Do you want to remove programs from the list? **NO**

IP address of this interface: **130.45.70.184**

Number of subnet bits: **0**

Userid/login name when accessing other hosts: **milgo**

Local host table [drive and pathname]: **C:\PCTCP**

Setting timezone info:

Offset from GMT [minutes: **300**

Timezone name: **EST**

IP address of default IP router (gateway):

---

**Note:** If the CMS 400 is connected to a network segment and needs to access other network segments, you need to enter the IP address for this default router.

---

Mail specific configuration:

Hostname of this machine: **milgo**

Domain of this host: **public**

Hostname (including domain) of mail relay:

### **Step 3: Installing CMS 400 software**

Install your CMS 400 as described in the *CMS 400 Installation Manual*.

---

**Note:** For additional information about PC/TCP or IBM's LAN Support Program, refer to the documentation that came with those products.

---

### **Step 4: Configuring Your CMS 400 Database**

Refer to the Configuration chapter of the *CMS 400 User's Guide* for details about creating or modifying the CMS 400 database, and for information about setting up the Network Map and various screen displays.

## **Configuring LIM**

With CMS 400 installed and the database created, you can configure the LAN Internetworking Manager. This involves:

- Discovering the IP devices (addresses) on your network
- Using SNMP community names
- Setting up general SNMP parameters
- Setting Proxy Agent Parameters
- Adding SNMP devices to the Network Map

## Discovering IP Devices

This procedure pings all devices in a range of user-entered IP addresses. A listing displays all IP addresses and the device types that responded to the pings. Any units not in the CMS 400 database will automatically be added.

To discover and automatically learn the SNMP units on the CMS 400 network, and their associated IP address(es), follow these steps:

1. Select Generic SNMP Control from the LAN Control menu.
2. Select Discover. The IP Address Scan Range window (Figure 1-1) appears.

IP Address Scan Range	
From	130.45.70.119
To	130.45.70.119
Channel	
Number Of Tries	3
Retry Interval (sec)	1
Require SNMP Reply	Y
Poll Addresses Cached In Units	Y

**Figure 1-1. IP Address Scan Range**

3. Fill in the fields of the IP Address Scan Range window according to Table 1-1.

**Table 1-1. IP Address Scan Range Fields**

Field	Enter the following
From	Enter the IP address you want to start with.
To	Enter the IP address you want to stop with.
Channel	Optional. Enter the name of an EDM channel to restrict the scan to the named channel. You can tab through this field to see a list of valid selections.
Number of Tries	The number of times CMS 400 will ping each address. The default is 3.
Retry Interval	The number of seconds between pings. The default is 1.
Require SNMP Reply	Y (yes) or N (no), if you want an SNMP reply message, or N (no) if not. Default is Y.
Poll Addresses Cached in Units	Y (yes) if do you want to poll the Address Cache of units in your selected range, or N (no) if not. Default is Y.

4. Press [PAGE DOWN].

Units responding that are not in the database are automatically added to the database.

## Using SNMP Community Names

CMS 400 lets you create “communities” of devices. By creating SNMP communities in a large distributed network, you can set up your network so that certain management stations are allowed to access certain SNMP devices in the named community. When you create a device in CMS 400, and you do not specify an SNMP community name, CMS 400 uses the default name “public.”

---

**Note:** You can add community names at any time. You do not have to define communities during the initial setup.

---

If you are planning on using Proxy Agents in your network, it's a good idea to assign the proxy-managed devices to a community name. When you set up your Proxy Agent parameters (described later in this chapter) you will be required to enter the Community Name, the Manager Address, the User Name, and the Group Name.

You can create up to 16 separate SNMP communities and associate each community with a particular site, group, subnet, or user. Only that site, group, subnet, or user has access to the community. For instructions about using CMS 400 to define sites, groups, and users, see the *CMS 400 User's Guide*.

To create up to 16 separate SNMP communities on the CMS 400 network:

1. Choose LAN Control from the CMS 400 Commands menu.
2. Select Generic SNMP Control. The Generic SNMP Control screen is displayed.
3. Select Communit from the Legend to display the SNMP Communities screen.
4. Enter a name that you want to associate with a specific site, group, subnet, or user, and press [ENTER].
5. Enter the name of the site, group, subnet, or user you want to associate with this community name in each of the appropriate fields. Enter information in any combination of these fields.
6. Press [PAGE DOWN] to accept the input. The SNMP community name is now used to identify the site, group, subnet, and user.

## Setting Up General SNMP Parameters

To set system-wide SNMP operating parameters across the CMS 400 network:

1. From the Main window, open the LAN Control menu and choose Generic SNMP. The Generic SNMP Control screen appears.
2. Select Gensetup from the legend at the bottom of the screen. The Systemwide Internetworking Parameters Window (Figure 1-2) appears.

Systemwide Internetworking Parameters	
Background Health Poll	Disable
SNMP No-Reply Timeout (sec)	3
Interval Between Background Pings (sec)	1
TFTP No-Reply Timeout (sec)	15
Permit TFTP Writes To Hub Disk	Enable
SNMP Proxy Agent	Enable
TRAP From Unknown Device Creates Unit	Y
Hub IP Address*	130.45.70.119
* This Parameter Is Only Accessible When PCTCP Is Not Installed (PPP only). If PCTCP Is Installed, It Determines The IP Address	

**Figure 1-2. Systemwide Internetworking Parameters**

3. Fill out the Parameters window:
  - In the Background Health Poll field, press [TAB] to disable or enable the background health poll.

- Enter the number of seconds for the SNMP No-Reply Time out to time out.
- Enter the number of seconds in the Interval Between Background Pings. To disable background pings, set the delay to zero.
- Enter the number of seconds in the TFTP No-Reply Timeout field.
- The Permit TFTP Writes To Hub Disk field lets you disable or enable the permission to write TFTP to a Hub disk.
- Enable or disable the SNMP Proxy Agent. If you enable, see the next procedure, Setting Proxy Agent Parameters.
- The Trap From Unknown Device Creates Unit field lets you specify whether or not you want to add an unknown device to your database.  
 If Y (yes) is selected, the system adds all unknown devices to your database.  
 If N (no) is selected, the system ignores all unknown devices and they are not added to your database.
- The Hub IP Address field shows the Hub's IP address.

---

**Note:** The Hub IP address is accessible only when TCP/IP is not installed (PPP only). If TCP/IP is installed, it determines the IP address.

---

4. After setting all the fields, press [PAGE DOWN] to accept the input.

## Setting Proxy Agent Parameters

If you enabled the SNMP Proxy Agent field, you will see the Proxy Agent Parameters window (Figure 1-3). This procedure describes how to set Proxy Agent Parameters. If you did not enable SNMP Proxy Agent, you will not see this screen and you can ignore this procedure.

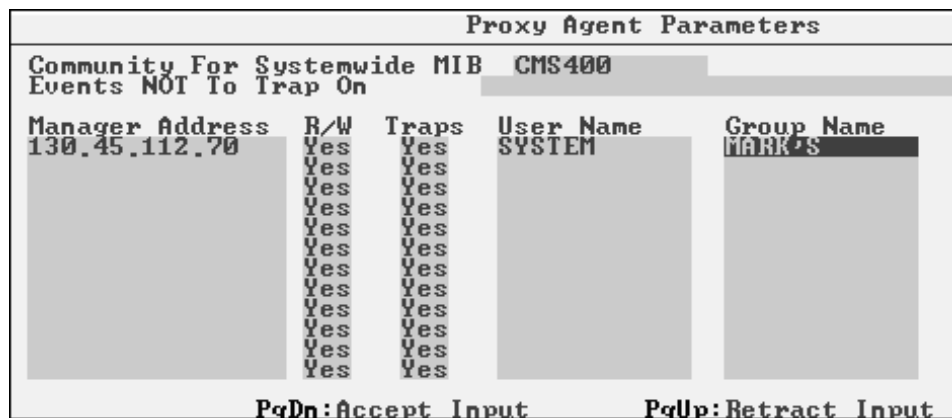


Figure 1-3. Proxy Agent Parameters Window

To set the parameters, follow these steps from the SNMP Proxy Agent Parameters screen:

1. Enter the name of the Community for Systemwide MIB.
2. Enter any events you do not want to trap on. Individual events can be separated by a colon (:), and event ranges can be entered. For example, (to enter events 6.1 through 6.5 enter 6.1-6.5).
3. Enter the User Name and the Group Name.
4. Press [PAGE DOWN].

## Adding Devices to the Network Map

To add a LAN internetworking device to CMS 400's Network Map:

1. Select Network Map from the Database Access menu.
2. Select Insert from the legend at the bottom of the screen. The Insert New Unit screen is displayed. For specific information about Network Map, see the *CMS 400 Reference Manual*.

Insert New Unit allows you to specify the following information for your SNMP device: a unique name, device type, diagnostic choice, and Internet (IP) address, if applicable (e.g., the INX5000 chassis does not require an IP address; it uses the IP address of the INX-NMM or INX-MGR installed in the chassis).

The diagnostic choice for the LAN internetworking devices is SNMP. To add the devices installed in the INX5000 and other SNMP network devices, use Discover (see "Discovering IP Devices" earlier in this chapter).

3. Once the device is defined in Network Map, verify that CMS 400 can communicate with it.
  - a. Place the cursor on the desired device in Network Map.
  - b. Select Poll from Network Map.

If CMS 400 can communicate with the device, the message: Target Device Responds to Poll is displayed. If it cannot communicate with the device, the message: Target Device Does Not Respond is displayed.



# Chapter 2

## SNMP Administration

---

### Overview

The CMS 400's LIM lets you customize SNMP MIBs. You can view existing MIBs, make changes to MIB files, and compile Abstract Syntax Notation One (ASN.1) files into MIBs.

Additionally, LIM offers an application tool that lets you create your own customized SNMP applications based on existing MIBs. (This application is detailed in Appendix B.) The tool lets you design your own application screen and select MIB objects to monitor within the custom application.

This chapter covers these types of SNMP administrative tasks. Setting up SNMP on the CMS 400 is described in Chapter 1 of this manual. Using SNMP to monitor and control your devices is described in Chapters 3 and 4.

### Assumptions

This chapter assumes that you have a working knowledge of SNMP and MIB files. You should understand the following:

- SNMP's dotted-decimal naming convention
- The five types of SNMP Protocol Data Units (PDUs)
- ASN.1 if you plan to write and compile your own MIBs

There are several reference books about SNMP, ASN.1, and MIB objects. Additionally, information is available about the Internet as *Requests for Comments* (RFCs). The following RFCs contain relevant information, and are available for downloading via FTP from ftp.nisc.sri.com as rfc/rfc####.txt (substitute a number in place of ####):

- RFC 1155 — SMI for TCP/IP-based Internets
- RFC 1157 — SNMP
- RFC 1212 — Concise MIB Definitions
- RFC 1213 — MIB II
- RFC 1215 — SNMP Traps

The RFC Index at the FTP site is continually updated. It lists all available RFCs and indicates when an RFC is replaced by an updated version.

## SNMP Procedures

This section includes the following SNMP administrative procedures:

- Viewing a MIB file
- Viewing a specific MIB object
- Adding a foreign SNMP device to the CMS 400 database
  - Adding a new device type to CMS 400 database
  - Adding the new device(s) to the Network Map
  - Compiling the device's MIB
  - Adding a MIB and associating it with the equipment
- Using health tables
  - Creating a health table
  - Associating LAN equipment with a health table
  - Modifying a health table
  - Deleting a health table
- Working with SNMP traps
  - Adding or modifying a trap
  - Masking a trap
  - Deleting a trap
  - Defining an alternate IP address for a trap
- Creating user-defined SNMP applications

### Viewing a MIB File

To display an SNMP MIB file:

1. Choose Database from the Commands menu.
2. Select Define SNMP MIB to display the Define MIB screen.
3. Click on the MIB file you want to view; it will appear highlighted.
4. Select Zoom from the Legend at the bottom of the screen.  
The first MIB object in the file appears on the screen. Use the [PAGE UP] and [PAGE DOWN] keys to scroll through the variable listing.

## Viewing a Specific MIB Object

To view a specific MIB object:

1. Choose Database from the CMS 400 Main menu.
2. Select Define SNMP MIB.
3. Select Find.
4. Enter either the Object Label or the Alias, or enter the Explicit Object ID number in the number fields.
5. Press [PAGE DOWN]. CMS displays the MIB, or reports that the MIB was not found.

## Adding a Foreign Device to the CMS 400 Database

To add a foreign device (one that does not have a Milgo MIB), you need to be at an independent hub workstation running in collapsed mode. This process assumes that you have the device's ASN.1 file ready for compiling. The process involves these basic steps:

- Adding the device type to the CMS 400 database
- Adding the new device(s) to the Network Map
- Compiling the device's ASN.1 file into a working MIB
- Adding the MIB and associating it with a device type

### Adding a Device Type to CMS 400

To add a new device type to the CMS 400 database, follow these steps from the Network Map screen:

1. Select Opt (Options) from the legend. This displays the Network Map Options screen (Figure 2-1).

Network Map Options			
Display Units By Unit Type	Display Autorefresh Enabled	First Key Legend Management	Alarm Color Display By Severity
Function Prompting Enabled	Units Not In Domain Show All	Channels Ordered By Alphabet	
Generic Unit Type Names			
Long	Short	Long	Short
NMS17 802.5	NMS_8025	NMS17 802.5	NMS_8025
NMS17 802.3	NMS_8023		

Figure 2-1. Network Map Options

2. Click on the first empty field under “Long,” and type in a long name for the unit (e.g., Proteon CNX500). You can use spaces in the long-name field.
3. Click on the corresponding Short name field and enter a short name (e.g., CNX500). The short name can be up to eight characters with no spaces allowed.
4. Press [PAGE DOWN] to add the device.

### Adding a New Device to the Network Map

To add the new device(s) to the Network Map, follow these steps from the Network Map screen:

1. Select Insert from the legend. This displays the Network Map Insert screen.
2. In the Unit Type field, enter the long name of the new unit. (You can make a wild card entry; for example, enter **pro\*** to bring up the Proteon CNX500 example.)
3. Press [PAGE DOWN].

### Compiling an ASN.1 File

To compile the ASN.1 file (provided by the device vendor), you need to make the file accessible to the CMS 400 workstation. Either insert the MIB diskette into a drive, or make sure the MIB file is copied onto the PC's hard disk.

To compile the ASN.1 file:

1. Select Define SNMP MIB from the Database menu. This displays the define SNMP MIB screen.

2. Select Compile. A window appears, prompting you to enter the full path of the ASN.1 file, and a short name to tag the resulting MIB file. This short name will appear in the MIB file list.
3. Enter the appropriate path and file name, and the short name.
4. Press [PAGE DOWN] to run the compiler.

### **Adding a MIB and Associating it with a Device Type**

To add a MIB file to the CMS 400 database, and to associate the MIB to a device:

1. Select Define SNMP MIB from the Database menu.  
This displays the Define SNMP MIB screen.
2. Select Add to bring up the Add/Assign window.
3. Enter the MIB name in the MIB Name field.
4. Enter up to six unit types in the Unit Type field. If you leave the Unit Type field blank, the MIB gets associated with all SNMP unit types.
5. Press [PAGE DOWN].

## **Using Health Tables**

The CMS 400 LIM Health Table is a set of up to four MIB objects with user-defined threshold settings. Once set up, these health tables can be associated with specific equipment. When thresholds are exceeded, alarms are generated in the CMS 400 Alarm screen. This section describes the following procedures:

- Creating a health table
- Associating LAN equipment with a health table
- Modifying a health table
- Deleting a health table

### **Creating a Health Table**

To create a health table:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select Generic SNMP Control to display the Generic SNMP Control screen.

3. Select Health from the screen legend to display the Health Control screen (Figure 2-2).
4. Select Add from the Health Control screen legend.

Health Checkup Name InterLan_227		Interval Between Checks 1 min	
Variable ifInOctets	Alarm If Beyond Thresholds: Lower	Instance Upper 555555555	No Autocancel Even If In Queue
Send Alarm A14	Text Octets Recv'd > 555M		
Variable sysDescr	Alarm If Beyond Thresholds: Lower	Instance Upper	No Autocancel Even If In Queue
Send Alarm	Text		
Variable sysDescr	Alarm If Beyond Thresholds: Lower	Instance Upper	No Autocancel Even If In Queue
Send Alarm	Text		
Variable sysDescr	Alarm If Beyond Thresholds: Lower	Instance Upper	No Autocancel Even If In Queue
Send Alarm	Text		
ESC:Done PgDn:Next PgUp:Prior A:dd M:odify D:elite			

**Figure 2-2. Health Control Screen**

5. Fill out the fields in the health table and press [PAGE DOWN] to accept input. (See Table 2-1).

**Table 2-1. Health Screen Field Definitions**

<b>Field Name</b>	<b>Field Definition</b>
Health Checkup Name	The name of the health table (up to 12 alphanumeric characters).
Interval Between Checks	The time between each poll.
Instance	The element you want to refer to if you have more than one element, (e.g. multiple power supplies).  The instance of a variable is included in the object identifier, a sequence of integers that represents the variable's place within the MIB.
Alarm if beyond thresholds	Generate an alarm if a number falls within or outside the upper or lower threshold. Valid selections are: Within or Beyond
Threshold Lower	The lowest value of the threshold.
Threshold Upper	The highest value of the threshold.
Send alarm	Enter text (up to 31 alphanumeric characters) that appears in the alarm screen when an alarm is generated.

Next, you need to associate the health table to specific equipment. See the next procedure, "Associating LAN Equipment with the Health Table."

### **Associating LAN Equipment with a Health Table**

To associate LAN equipment with a health table:

1. Open the Network Map and place your cursor inside the unit you want to associate with a health table.
2. Select Mod (Modify) from the screen legend.
3. Put your cursor in the Health Table field.
4. Press [TAB] until the health table name appears.
5. Press [PAGE DOWN].
6. From the LAN Control menu, open the Generic SNMP Control screen.
7. Select Gen-Setup.
8. Make sure the Background SNMP Object Health Poll is enabled.

9. Press [PAGE DOWN].

Alarms generated as a result of the health table can be viewed in the Alarms screen.

### **Modifying a Health Table**

To modify a health table:

1. Select Generic SNMP Control from the LAN Control menu.  
The generic SNMP control is displayed.
2. Select Health. This displays the Generic SNMP Health Control screen.
3. Select the health table you want to modify.
4. Select Modify. Make the appropriate changes.
5. Press [PAGE DOWN].

### **Deleting A Health Table**

To delete a health table:

1. Select Generic SNMP Control from the LAN Control menu.
2. Select Health. The Generic SNMP Health Control screen is displayed.
3. Select the health table you want to delete.
4. Select Delete. You will be prompted to confirm the deletion.
5. Type **Y** to delete the table.

## **Working With SNMP Traps**

This section covers SNMP's Enterprise-Specific Trap. You should have working knowledge of SNMP traps. Refer to RFCs 1157 and 1215. Also, when referencing traps, refer to vendor-provided documentation that defines and describes the unit's enterprise-specific numbering scheme.

The procedures described in this section include:

- Adding or modifying a trap
- Masking a trap in the CMS 400

- Deleting a trap
- Defining an alternate IP address for a trap

### Adding or Modifying a Trap

To add or modify a trap:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select Generic SNMP Control.
3. Select Traps from the screen legend.
4. Select Add to display the Add/Modify A Trap Definition screen (Figure 2-3).

Add/Modify A TRAP Definition	
Label	<input type="text"/>
Enterprise	<input type="text"/>
TRAP Type	6:enterprise Specific 0
Alarm Type	SRQ
Discard	N
Bindings	<input type="text"/>
Description	This TRAP is generated whenever.... <input type="text"/>
PgDn:Accept Input      PgUp:Retract Input	

**Figure 2-3. Add/Modify Trap Definition Screen**

5. Fill out the Add/Modify Trap Definition screen by entering:
  - The name of the trap label
  - The name of the Enterprise label
  - The name of the trap type
  - The specific trap type number
  - The alarm type

- **Y** (yes) or **N** (no) in the Discard field
  - The Bindings comments
  - Description of the trap
6. Press [PAGE DOWN] and then [ESC] to return to the Generic SNMP Control Screen.

After a trap is defined, it needs to be “masked” to the CMS 400. For details, see the next procedure.

### Masking a Trap in the CMS 400

After a trap has been added, it must be masked in the CMS 400 to take effect.

To mask a trap:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select Generic SNMP Control to display the Generic SNMP control screen.
3. Select Traps to display the Trap Control.
4. Select Masking to display the Traps to Mask screen.

TRAPs To Mask <a,b,b-b, ..z.z>	Unit Type	Site	Group
2-6	Generic Type 1		

PgDn: Accept Input      PgUp: Retract Input

**Figure 2-4. Traps to Mask Screen**

5. Fill out the Traps to Mask screen by entering:
  - The mnemonic number of the trap(s) you want to mask in the Traps To Mask field (e.g., 6.2, 6.5-6.8, etc). You can enter more than one trap at a time.
  - The unit type name you want to mask in the Unit Type field.

- The unit site name you want to mask in the Site field.
  - The unit group name you want to mask in the Group Type field.
6. Press [PAGE DOWN].

### **Deleting a Trap**

To delete a trap:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select Generic SNMP Control.
3. Select Traps to display the Trap Control screen.
4. Select the trap you want to delete.
5. Select Delete. You are prompted to press **Y** (yes) to confirm, or any other key to cancel the deletion request.

### **Defining an Alternate IP Address for a Trap**

To define an alternate IP address that a trap is reported to:

1. Select Generic SNMP Control from the LAN Control menu.
2. Select Traps to display the Trap Control screen.
3. Select IP-Adds to identify the Alternate IP addresses for each unit.
4. Enter the unit name and IP address of the alternate unit and press [PAGE DOWN].

For additional information about trap numbers and descriptions for: RNX6100, RNX6150, RNX6200, RNX6400, RNX6500, and RNX6600 modules, refer to your *Proteon Event Logging System Messages Guide*, Doc. No. 42-040209-00.

For additional information about trap numbers and descriptions for: INXNMM, INXNTS, INX4000L, INX4000R, INX400L, INX400R, and INXNTS200 modules, refer to your *Milgo MIB Reference Manuals*.

For additional information about trap numbers and descriptions for: EAN 4000 and SR 4200 modules, refer to your *Sync Research Frame Node NMS Command Reference Guide*, and *ConversionNode User's Guide*.

For additional information about trap numbers and descriptions for: SNMP, refer to your *Internet Specification*, Doc. No. RFC1157 and RFC1215.

## Creating User-Defined SNMP Applications

You can build your own user-defined applications with LIM's Define SNMP Application feature. The feature lets you draw your own user interface, and access MIB variables throughout the network.

Applications are saved in files with an .APP extension and a name that begins with a dollar-sign (\$).

### Adding an SNMP Application

Building an SNMP application takes planning and general knowledge of the LIM application tool. This procedure is meant to serve as a reference for users who have some experience or basic training using the SNMP Application feature. If you're new to this feature, see Appendix B, "Define SNMP Applications: A Tutorial."

To add an SNMP application:

1. Choose Applications from the CMS 400 Main menu.
2. Select Define SNMP Application to display the Select An Operation screen.
3. Select Add Application. The application name prompt is displayed.
4. Enter a descriptive name.

You can invoke the application by entering its name on the command line. Or, you can select it from a menu within the Custom SNMP Application. To specify the name as an argument, enter: **SNM\_APP APP=\$name**.

5. Select Setup to set up general options for the application, including titles on of the window frames, how many units to prompt for as target units, and how many seconds between screen updates.
6. Select Backdrop to design a page background. Table 2-2 explains the backdrop level fields.

**Table 2-2. Custom SNMP Application Field Definitions**

<b>SNMP Field Name</b>	<b>SNMP Field Definition</b>
Color	Sets the default background and foreground colors.
Text-Mode	Allows direct text entry at the current cursor position.
Line-Mode	Allows direct entry of line-drawing characters.
Box-Mode	Allows blank boxes and outlined boxes to be drawn, and cut-and-paste operations on boxed areas.
Flood	Fills the color around the current cursor with the current default background color.
Erase	Clears the page to the current default background color.
Escape	Finishes the backdrop edit session and allows all changes to be revoked.

7. Select Items to add, modify, delete, or position one or many items. An item may represent: a polled SNMP value as a LED, gauge or explicit text; a button to cause an action such as a page change or function invocation; or a text string, such as the name of the target device.

Add and Modify display a common screen of item parameters. Table 2-3 explains the Item Definition fields.

8. Select General. A General Applications Parameters screen is displayed.
- a. Enter the long application name, the short application name, and the target unit selection.
  - b. In the Target Unit Selection, choose: Prompt For One Unit, Prompt For Many Units, or Use Item Specified Units.
9. Press [ESC] to cancel the Add function. The Define SNMP Application menu is redisplayed.

**Table 2-3. Item Definition Fields**

Item Field Name	Item Field Definition
Type of Item	Specify how an item appears. Press [TAB] to select the type of Item (LED, gauge, button, and so on).
Color	Select a color default of your foreground and background. Press [TAB] to select the following colors: white, black, blue, green, cyan, red, magenta, and yellow.
Red On Alarms	Select what (if anything) to turn red if alarms are in the queue. Press [TAB] to select the following: no, fore, back, and both.
Positions/Size	Select the row, column, height, and width of an item. Press [TAB] to select the following values: 1 through 25.
Action When Zoomed	Select an action item (if any) when zoomed. Press [TAB] to select the page to zoom to.
Page To Zoom To	Select an application page (if any) to change to when zoomed. Press [TAB] to select the page to zoom to.
Function To Invoke	Select a CMS function or script (if any) to initiate by pressing [TAB].
Poll For MIB Object	Poll a unit when a page is painted, at each page update, or not at all. Press [TAB] to select: never, ignore MIB object, when page is first painted, or every screen update.
Analysis	Represent a polled value; raw or per second.
MIB, Object and Instance	Use an SNMP variable to poll from unit. You may select several choices of MIB, object and instance to poll from. Select choices by pressing [TAB].
Unit to Represent	Select many target units to represent. Press [TAB] to select 1 through 16.
Blank If Chosen	Don't show item if unit is not selected. Use the token <i>%un</i> to represent a unit in the command line, where <i>n</i> is 1-16 for one of the selected target units or 0 for the fixed unit, (e.g. DIS ALA UNI=%U1). Select choices by pressing [TAB].
Fixed Unit Choices	Ignore target units and represent this unit. Select choices by pressing [TAB].
Button Label	Add a 16-character text label on a button item.
Gauge Range	Add an 8-character range of from and to values for a gauge item.
Indicator Color	Have up to four different color changes based on thresholds. Press [TAB] to select the following colors: blue, green, cyan, red, magenta, yellow, white, and black.

## Modifying an SNMP Application

To modify an SNMP application:

1. Select Define SNMP Applications from the Applications menu. The Select An Operation screen is displayed.
2. Select Modify Application. An application name is displayed in a prompt field.
3. Select an application by pressing [TAB] to display the application you want to modify.
4. Press [PAGE DOWN]. The application is displayed.
5. You may now modify the application. Refer to Add for a detailed description of the fields.
6. Press [PAGE DOWN].

## Deleting an SNMP Application

To delete an SNMP application:

1. Select Define SNMP Applications from the Applications menu. The Select An Operation screen is displayed.
3. Select Delete Application. An application name is displayed in a prompt field.
4. Press [TAB] to display the application you want to delete.
5. Press [PAGE DOWN]. You are prompted to confirm.
6. Type **Y** (yes) to confirm or any other key to cancel.

## Renaming an SNMP Application

To rename an SNMP application:

1. Select Define SNMP Applications from the Applications menu. The Select An Operation screen is displayed.
2. Select Rename Application. An application is displayed in a prompt field.
3. Press [TAB] to display the application you want to rename.
4. Press [ENTER]. This displays the Desired Name field.
5. Type in the new name and press [ENTER].

6. Press [PAGE DOWN]. You are prompted to confirm.
7. Press Y (yes) to confirm, or any other key to cancel.

### **Displaying a Menu of Your SNMP Applications**

The Custom SNMP Application provides you with a menu of all the SNMP applications built with the Define SNMP application function. If you have too many applications to fit into a menu, applications are displayed in a prompt field. Choices can be viewed and selected by pressing [TAB].

### **Configuring a Custom SNMP Application**

To configure a custom SNMP Application:

1. Select Custom SNMP Applications from the Applications menu. The Select An Application screen is displayed.
2. Select an application.
3. Enter the unit information and press [PAGE DOWN]. The Configure screen presents a list of unit values. You can select, display and modify one unit values. Also, you can use the define SNMP Application function to define the choices in the list of unit values.

# Chapter 3

## Configuring LAN Equipment

---

### Introduction

This chapter describes the functions for configuring specific SNMP equipment. For information about configuring the CMS 400 and the LIM, see Chapter 1, “Getting Started.” For information on configuring specific SNMP devices, see Chapter 2, “SNMP Administration.”

This chapter includes the procedures for configuring the following equipment:

- INX5000
  - Configuring devices in the chassis
  - Adding units to the chassis
  - Modifying units in the chassis
  - Deleting INX5000 units
  - Moving internal Ethernet buses
- INX Managed 10BaseT Repeater
  - Using the filtered repeater
  - Changing the names of a repeater
  - Changing alarm thresholds
- INX Network Terminal Server
  - Modifying operating parameters
  - Configuring a port
  - Changing module names
  - Changing module thresholds
- INX T-Ring CAU
  - Configuring a port
  - Changing the name of a CAU
  - Changing alarm thresholds
- INX 4000 Bridge
  - Changing the bridge name
  - Configuring a port
  - Configuring operating parameters
  - Changing alarm thresholds

- RNX6x00/6150 Bridge/Router
  - Configuring the RNX6x00/6150
  - Configuring the console
  - Editing the handler definition file
  - Adding units to the RNX6300 console database

## INX5000 Configuration

This section includes the following procedures for the INX5000:

- Displaying an INX5000 device
- Configuring devices in the chassis
- Adding units to the chassis
- Modifying units in the chassis
- Deleting INX5000 units
- Moving internal Ethernet buses

### Displaying a Device in the INX5000 Chassis

INX5000 configuration procedures usually begin at the specific device screen. This procedure describes how to get to the device screen for display and configuration purposes:

1. Choose LAN Control from the CMS 400 Commands menu.
2. Select Generic SNMP Control.
3. Select the INX5000 chassis.

### Configuring Devices in the INX5000

This procedure allows you to set a single MIB variable in a unit. All MIB variables displayed using Configure have read/write status.

To configure an INX5000 device, bring up the device screen for the unit you want to configure, and follow these steps:

1. Select Configure to display a list of MIB files.
2. Select a MIB file and press [PAGE DOWN].

3. Press [ENTER] until the cursor is next to the MIB variable you want to set, or [PAGE DOWN] to view more selections.
4. Press [TAB]. The system prompts for a specific instance.
5. Press [ENTER] to see the variable's current value and a prompt to change the variable.
6. Make the appropriate change.
7. Press [PAGE DOWN] .
8. Press any key to continue. The configuration is completed.

### **Adding Units to the Chassis**

To add units in the INX5000 chassis slots to the CMS 400 database without using the Network Map:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select INX5000 Hub Control.
3. Enter the name of the INX5000 and press [PAGE DOWN].
4. Type [>] to view additional selections.
5. Select Database to display the Select An Operation screen.
6. Select Add. The Card Definition screen is displayed.
7. Enter the unit name, IP address, module type, and slot number, and press [PAGE DOWN].

### **Modifying Units in the Chassis**

To modify units in the INX5000 chassis slots to the CMS 400 database, follow these steps from the INX5000 unit screen:

1. Select Modify. The Card Definition screen is displayed.
2. Make the appropriate changes.
3. Press [PAGE DOWN]. You are prompted to make this card the current controller.
4. Press [PAGE DOWN] again. The card is now the controller. This setting is saved in the database.

---

**Note:** The “current controller” prompt is not displayed if the current card is already the controller, or is the only controller available. The prompt applies only to cards with control capability.

---

### Deleting INX5000 Units

To delete INX5000 units from the CMS 400 database, follow these steps from the unit screen:

1. Select Delete. The following prompt is displayed: Are You Certain? Press Y to Confirm, Any Other to Cancel.
2. Press **Y** to confirm.
3. Press [PAGE DOWN].

### Moving Internal Ethernet Buses

You can move a CMM off of a bus. Also, you can move the connectivity module (AUI/FST) of the CMM off of a bus. If an NMM connectivity module is not disabled, you can move the connectivity module (AUI/FST) of the NMM to a bus with an enabled AUI/FST.

To move a selected module from one bus to another on the INX5000 chassis, follow these steps from the unit screen:

---

**Note:** Relocation of cards to different buses can cause network problems.

---



---

**Caution:** Use this operation to relocate a card on a different bus only if you are very familiar with the internal architecture of the INX5000.

---

1. Place the cursor on the module to be moved.
2. Select Move. The following prompt is displayed: Are You Certain?
3. Press **Y** to move the module to the other bus.

## INX Managed 10 Base T Configuration

This section includes the following configuration procedures for the INX 10 Base T Repeater:

- Using the filtered repeater
- Changing the names of a repeater
- Changing alarm thresholds

### Using the Filtered Repeater

To filter the selected INX Managed 10 Base T:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select INX Managed Repeater Control.
3. Enter the name of the INX Managed 10 Base T that you want to access, and press [PAGE DOWN].
4. Select Filter from the screen legend. The INX Managed 10 Base T Filtered Repeater Management screen is displayed.
5. Select Configure. The INX Managed 10 Base T Configuration screen is displayed.
6. Select Bus. The statistics from the internal bus side of the filter is displayed. This screen is view-only.
7. Select Userport. The statistics from the user port side of the filter is displayed. This screen is view-only.
8. Select Packets. You are prompted to enter the filtering mode.
9. Press [TAB] to select Learn or Security. You can also add or delete the packets.
10. To add a packet, select Add. You are prompted to add a four-digit packet number.
11. Type the new number. A new packet is created.
12. To delete a packet, select Delete.

### **Changing the Names of a Repeater**

To change the domain name, contact name, and location of a selected INX Managed 10 Base T Repeater, follow these steps:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select INX Managed Repeater Control.
3. Enter the name of the INX Managed 10 Base T that you want to access, and press [PAGE DOWN].
4. Select Names. The cursor moves to the Domain Name field.
5. Make the appropriate changes.
6. Press [PAGE DOWN].

### **Changing Alarm Thresholds**

To specify thresholds for specific INX Managed 10 Base T MIB variables and generate alarms when the values exceed the specified limits:

1. Select INX Managed Repeater Control from the LAN Control menu.
2. Enter the name of the INX Managed 10 Base T that you want to access and press [Page Down].
3. Type [>] or click on the > at the far right of the screen legend.
4. Select Thresholds to display the INX Managed 10 Base T Threshold screen.
5. Select Add.
6. Fill out the threshold screen by entering:
  - category
  - MIB object
  - number of the instance
  - "Rises Above" or "Falls Below"
  - the value that the count must recede by before another alarm is generated
  - the IP address of the device where the alarm will be sent
  - the community name associated with the alarm
7. Press [PAGE DOWN] to accept the input.

To modify a threshold:

1. Use [PAGE UP] and [PAGE DOWN] to display the threshold you want to modify.
2. Select Modify and follow the Add procedure to change the fields.

To delete a threshold:

1. Use [PAGE UP] and [PAGE DOWN] to display the threshold you want to delete.
2. Select Delete. The system displays the following prompt: Are You Certain? Press Y to Confirm, Any Other to Cancel.
3. Press Y to delete the threshold.

## INX NTS Configuration

This section includes the following configuration procedures for the INX Network Terminal Server (NTS):

- Modifying operating parameters
- Configuring a port
- Changing module names
- Changing module thresholds

### Modifying Operating Parameters

To display and modify operating parameters for a selected INX-NTS

1. Choose LAN Control from the CMS 400 Main menu.
2. Select INX-NTS Control.
3. Enter the name of the INX-NTS and press [PAGE DOWN].
4. Select Examine. The system displays an INX-NTS screen.
5. Select Modify to change the operating parameters of the selected INX-NTS. The field definitions for the INX-NTS Examine screen are described in Table 3-1.
6. Press [PAGE DOWN].

**Table 3-1. INX-NTS Screen Field Definitions**

<b>Field Name</b>	<b>Field Definition</b>
Sign-on Text	Text that appears when you are in command mode.
Prompt Text	Command-mode prompt that appears when you are connected to an INX-NTS.
Term Domain Name	The name appended to the host name when the INX-NTS requests a name server and the string entered by the user contains no period. (If the string does contain a period, the INX-NTS assumes it is a fully qualified domain name.)
Up-Time Node Name	The node name to be contained in future RWHO (UPTIME) broadcasts. The name can contain up to seven characters.
Buffer Count	Maximum number of buffers a Telnet, RLOGIN, X server, or LAT process can use for inbound traffic. Valid values are 2, 3, 4.
Read Buffer Size	Number of bytes used by each read buffer. Buffer size should be a factor of the TCP window size. For example, if the TCP window size is 512, the buffer size is best set at 256.
Write Buffer Size	Number of bytes that each buffer can use for outbound traffic. Buffer size should be a factor of the TCP window size. For example, if the TCP window size is 512, the buffer size should be set at 128 or 64.
TCP Window Size	Number of read buffers, multiplied by the size of the read buffers. Maximum is 1024. This parameter specifies the maximum number of bytes that the connection is able to accept.
TCP Max Segment	Maximum number of bytes that the INX-NTS expects to receive in a packet of data. Use a protocol analyzer to determine the maximum number of bytes. For best performance, the TCP segment size should be a factor of the TCP window size.
TCP Ack Time <ms>	Maximum acknowledgment time between TCP protocol packets required for the INX-NTS TCP implementation. The range is 50-300 milliseconds.

### Configuring a Port

To configure a single port for a selected INX-NTS:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select INX-NTS Control.
3. Enter the name of the INX-NTS and press [PAGE DOWN].
4. Position the cursor on the port you want to select.
5. Select Config-Port. The INX-NTS Port Configuration screen is displayed

---

**Note:** The first session, active session, current sessions, maximum sessions, Rx characters, and Tx character fields are view-only.

---

6. After you have finished entering the configuration parameters for the port, press [PAGE DOWN] to accept the input.

Table 3-2 lists the field definitions for the INX-NTS Port Configuration screen.

**Table 3-2. INX-NTS Port Configuration Field Definitions**

Field Name	Field Definition
RX Speed	The baud rate for data received by the port, expressed in bits per second (bps). If you want the INX-NTS to automatically determine baud rates, press [TAB] until Autobaud appears in the field. The default baud rate is 9600. Valid values are Autobaud, 110, 300, 600, 1200, 2400, 4800, 9600, 19200, and 38400.
TX Speed	The baud rate for data transmitted by the port, expressed in bits per second (bps). If you want the INX-NTS to automatically determine baud rates, press [Tab] until Autobaud appears in the field. The default baud rate is 9600. Valid values are Autobaud, 110, 300, 600, 1200, 2400, 4800, 9600, 19200, and 38400.
Parity	Enter a value for parity that matches the setting on the device attached to the INX-NTS port.
Data Bits	Number of bits in each character transmitted between the INX-NTS port and an attached device. Enter a value that matches the setting of the device attached to the port.
Modem Control	This parameter determines the use of the modem control RS-232 signals. Enter a value that matches the setting of the attached device.
RX Flow Control	The mechanism that the INX-NTS port is to use to hold off data from its attached device if its buffers are becoming full. Valid values are None, Hardware, Handx, and Xon/Xoff.
TX Flow Control	The mechanism that the attached device is to use if the device wants to stop data coming from the INX-NTS port. Valid values are None, Hardware, Handx, and Xon/Xoff.

**Table 3-2. INX-NTS Port Configuration Field Definitions (Continued)**

Field Name	Field Definition
Use Ring Indicator	This parameter determines the use of the Ring Indicator (RI) RS-232 signal. Press [TAB] to toggle between Yes and No. If you have set modem control to DCE, this field must be set to No. If you have set modem control to DTE, Yes means that the INX-NTS port will use the RI signal, and No means the signal will not be used.
Password	The password needed to connect to the port. Enter a password of up to seven characters.
Abort Character	Enter the character you want the user to use to suspend output to the screen for a current process.
Interrupt Character	Enter the character you want the user to use to kill a current process on the host machine.
Inactive Timeout	The number of minutes that a port can be inactive before the INX-NTS closes all existing virtual circuits on that port. The Timeout range can be from 1 to 255. This feature works on all ports except for permanent. To disable the inactivity Timeout function, set this field to 0.
Inactive time left	The number of minutes left before the inactivity timer (see the previous field, Inactive Timeout) expires, and all virtual circuits for this port are closed. Setting this variable to 0 temporarily disables the inactivity timer, so virtual circuits are maintained as long as the port remains inactive. When port activity resumes, however, the inactivity timer is reactivated.
Suppress software msgs	Press [TAB] to toggle between Yes and No. Yes configures a port so that it suppresses the sending of all messages generated by the LAT/TCP software.
Function	Press [TAB] until the port type you want appears in the field. Valid values are Terminal (if you are attaching a terminal to the INX-NTS port), Perm Ckt (to establish a permanent virtual circuit to some other network source), Both (to configure a port to accept and request connection with other network resources), Demand Ckt (to set up a demand virtual circuit with other network resources), and Queue (to configure a port to accept and hold requests).
State	This field allows you to enable or disable the port. Press [TAB] to toggle between enable and disable.
XON character	This field allows you to enter an XON character to be used to resume output to the screen. Enter the hex value corresponding to the ASCII code for the character you want to use.

**Table 3-2. INX-NTS Port Configuration Field Definitions** (Continued)

Field Name	Field Definition
XOFF character	This field allows you to enter an XOFF character to be used to halt output from the INX-NTS to the screen. Enter the hex value corresponding to the ASCII code for the character you want to use.
Server Port	The TCP port number that this serial port uses when listening for Telnet connections. If this port is not configured to listen for inbound connection requests, this variable returns 65535. The default TCP port number is 23.

### Changing Module Names

To change the domain name, contact name, and location of a selected INX-NTS module:

1. Select INX-NTS Control from the LAN Control menu.
2. Enter the name of the INX-NTS and press [PAGE DOWN].
3. Type [>] or click on the > at the far right of the screen legend.
4. Select Names. The cursor moves to the Domain Name field.
5. Make the appropriate changes and press [PAGE DOWN].

### Changing Module Thresholds

To specify thresholds for specific INX-NTS MIB variables and generate alarms when the values exceed the specified limits, follow these steps:

1. Select INX-NTS Control from the LAN Control menu.
2. Enter the name of the INX-NTS and press [PAGE DOWN].
3. Type [>] or click on the > at the far right of the screen legend.
4. Select Thresholds. The INX-NTS Threshold screen is displayed.

From the INX-NTS Threshold screen, you can add, modify, and delete thresholds.

To add a threshold:

1. Select Add.
2. Fill out the threshold screen by entering:
  - category

- MIB object
- number of the instance
- "Rises Above" or "Falls Below"
- the value that the count must recede by before another alarm is generated
- the IP address of the device where the alarm will be sent
- the community name associated with the alarm

3. Press [PAGE DOWN].

To modify a threshold:

1. Use [PAGE UP] and [PAGE DOWN] to display the threshold you want to modify.
2. Select Modify and follow the Add procedure to change the fields.

To delete a threshold:

1. Use [PAGE UP] and [PAGE DOWN] to display the threshold you want to delete.
2. Select Delete. The following prompt is displayed: Are You Certain? Press Y to Confirm, Any Other to Cancel.
3. Press **Y**.

## **INX Token Ring CAU Configuration**

This section includes the following configuration procedures for the INX Token Ring CAU:

- Configuring a Port
- Changing the Name of a CAU
- Changing Alarm Thresholds

### **Configuring a Port**

To configure a single INX T-Ring CAU port:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select INX T-Ring CAU.
3. Enter the name of the INX T-Ring CAU and press [PAGE DOWN].

4. Position the cursor on the port you want to select.
5. Select SNMP to bring up the list of MIB files.
6. Select the MIB file.
7. Select Configure.

---

**Note:** The first session, active session, current sessions, maximum sessions, Rx characters, and Tx character fields are view-only.

---

8. Make the appropriate entries and press [PAGE DOWN].

### **Changing the Name of a CAU**

To change the domain name, contact name and location of a selected INX T-Ring CAU:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select INX T-Ring CAU.
3. Enter the name of the INX T-Ring CAU and press [PAGE DOWN].
4. Select Names. The cursor moves to the Domain Name field.
5. Make the appropriate changes and press [PAGE DOWN].

### **Changing Alarm Thresholds**

To specify thresholds for a specific INX T-Ring CAU MIB variable and generate alarms when the values exceed the specified limits:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select INX T-Ring CAU.
3. Enter the name of the INX T-Ring CAU and press [PAGE DOWN].
4. Type [>] or click on the > at the far right of the screen legend.
5. Select Thresholds. The INX T-Ring CAU Threshold screen is displayed.
6. Select Modify.
7. Fill out the threshold screen by entering:
  - category
  - MIB object

- number of the instance
- "Rises Above" or "Falls Below"
- the value that the count must recede by before another alarm is generated
- the IP address of the device where the alarm will be sent
- the community name associated with the alarm

8. Press [PAGE DOWN].

To delete a threshold:

1. Use [PAGE UP] and [PAGE DOWN] to display the threshold you want to delete.
2. Select Delete. The following prompt is displayed: Are You Certain? Press Y to Confirm, Any Other to Cancel.
3. Press **Y** to delete the threshold.

## **INX 4000 Bridge Configuration**

This section includes the following configuration procedures for the INX 4000 Bridge:

- Changing the Bridge Name
- Configuring a Port
- Configuring Operating Parameters
- Changing Alarm Thresholds

### **Changing the Bridge Name**

To change the domain name, contact name and location of a selected INX4000 bridge:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select INX4000 Bridge Control.
3. Enter the name of the INX4000 Bridge and press [PAGE DOWN].
4. Select Names. The cursor appears in the Domain Name field.
5. Make the appropriate changes and press [PAGE DOWN] to accept the input.

## Configuring an INX4000 Port

To configure one of the LAN ports on the INX4000/L or one of the LAN or WAN ports on the INX4000/R:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select INX 4000 Bridge Control.
3. Enter the name of the INX 4000 and press [PAGE DOWN].
4. Position the cursor on the port you want to select.
5. Select Config-Port. The INX 4000 Port Configuration screen is displayed.
6. After you finish entering the configuration parameters for the port, press [PAGE DOWN] to accept the input.

Table 3-3 lists the field definitions for the INX 4000 Port Configuration screen.

7. After you have finished entering the configuration parameters for the port, press [PAGE DOWN] to accept the input.

**Table 3-3. INX4000 Port Configuration Screen Field Definitions**

Field Name	Field Definition
Transmit on CRS	When set to 1, transmission occurs even if carrier sense is not detected on the channel in question. When set to 2, transmission occurs only if carrier sense is detected.
Broadcast RX	When set to 1, broadcast frames are received on this channel. When set to 2, broadcasts are ignored.
Path Cost	Path cost for the specified port.
Spanning-Tree State	Valid values are: disabled (1), blocking (2), learning (3), forwarding (4), and listening (5).
Port Priority	The spanning-tree port priority of this port.
Default Priority	The default spanning-tree priority of the port. This value is stored in NVRAM and is the priority when the bridge powers up.
Designated Root	Physical address of the root bridge for the spanning-tree network. Enter the address of the root bridge.
Designated Cost	Cost of the path to the root bridge from the designated port.

**Table 3-3. INX4000 Port Configuration Screen Field Definitions (Continued)**

Field Name	Field Definition
Designated Port	Port nearest the root bridge for the network to which the specified port is attached.
Designated Bridge	Bridge that contains the root port for the network to which the specified port is attached.
Topology Change Ack	Number of times the topology change flag for the bridge has been reset since the INX4000 bridge was last initialized.
Identifier	Bridge with the lowest bridge identifier value, which becomes the root bridge.

### Configuring Operating Parameters

To configure the general operating parameters of the INX4000 bridge:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select INX 4000 Bridge Control.
3. Enter the name of the INX 4000 and press [PAGE DOWN].
4. Select General to display the General Bridge Parameters screen. The values that appear in red may be modified.

Table 3-4 lists the field definitions for the General Bridge Parameters screen.

5. After you finish entering the general operating parameters for the bridge, press [PAGE DOWN] to accept the input.
6. Press [ESC] and the system redisplay the standard Unit Criteria Selection screen.

**Table 3-4. General Bridge Parameters Field Definitions**

Field Name	Field Definition
Bridge Mode	Used to specify the performance state of the bridge. Press [TAB] until the mode you want appears in the field. Valid modes are: Forward, Relay, Security, and Listen.
Default Bridge Mode	Used to specify the default performance state of the bridge. Press [TAB] until the mode you want appears in the field. Valid modes are: Forward, Relay, Security, and Listen.
Filter Matches	Allows you to specify which action the bridge should take if an incoming frame's address matches an entry in the range table. Press [TAB] until the option you want appears in the field. Valid options are: Pass, Discard, and Disable.
Span-Tree Mode	Allows you to enable or disable the Spanning Tree algorithm. Press [TAB] to toggle between Enable and Disable.
Default Span-Tree Mode	Allows you to enable or disable the default Spanning Tree algorithm. Press [TAB] to toggle between Enable and Disable.
Span-Tree Hello timer	Amount of time that (in seconds) the root bridge waits between issuing hello messages. Valid values are 1 through 10.
Default Hello Timer	Amount of time that (in seconds) the root bridge waits between issuing hello messages. This variable sets the default value for this parameter. Valid values are 1 through 10.
Hold Time	The time, (in seconds) after which unacknowledged hello messages are re-sent.
Span-Tree Version	The spanning-tree protocol currently being run on the module.
Default Version	Allows you to select the version of the spanning-tree protocol to run. Press [TAB] to toggle between Rev 8 and Rev C. All bridges in the same spanning-tree domain must run the same spanning tree protocol version.
Maximum Age	The longest period of time (in seconds) that a hello message generated by a bridge remains on the network. After this period of time, the packet times out and is discarded.
Default Maximum Age	This is the longest period of time a hello message generated by a bridge remains on the network. After this period of time, the packet times out and is discarded. Enter a value between 6 and 28 (seconds). This variable sets the default value for this parameter.

**Table 3-4. General Bridge Parameters Field Definitions (Continued)**

Field Name	Field Definition
Live Forward Delay	The current forward delay set for the bridge on the network, which is dictated by the root bridge's setting for this parameter. The forward delay is the number of seconds that the bridge stays in preforwarding (listening) mode before it goes into forwarding mode.
Bridge Forward Delay	The forward delay set for the bridge on the network, which is dictated by the root bridge's setting for this parameter. If this bridge is the root bridge, this value is the forward delay used by all bridges in the network.
Default Forward Delay	The value of the forwarded delay parameter set in this bridge's NVRAM. This variable sets the default value for this parameter; this value is stored in NVRAM and is used while the spanning-tree algorithm is configuring the network.
Topology Change Count	The number of times that the topology change flag has been reset since the bridge was last initialized.
Live Hello Timer	The amount of time, (in seconds) that an INX4000 waits between issuing hello messages. This value is the same as the initial hello time used by the root bridge.
Live Maximum Age	The bridge's setting for maximum age when it is the root, or during a spanning-tree configuration change, when it is attempting to become the root.
Default Hold Time	The time, (in seconds), after which unacknowledged hello messages are resent. This is also the value stored in NVRAM. It is used to initialize Hold Time when the bridge is powered up.
Priority	This is the current spanning-tree priority of the bridge.
Default Priority	This is the default spanning-tree priority of the bridge. This value is stored in EEPROM and copied into NVRAM. It is the value the bridge will use the next time it powers up.

### Changing Alarm Thresholds

To specify thresholds for specific INX4000 bridge MIB variables and generate alarms when the values exceed the specified limits:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select INX 4000 Bridge Control.
3. Enter the name of the INX 4000 and press [PAGE DOWN].

4. Type [>] or click on the > at the far right of the screen legend.
5. Select Thresholds. The INX4000 bridge threshold screen is displayed.
6. Select Modify.
7. Fill out the threshold screen by entering:
  - category
  - MIB object
  - number of the instance
  - “Rises Above” or “Falls Below”
  - the value that the count must recede by before another alarm is generated
  - the IP address of the device where the alarm will be sent
  - the community name associated with the alarm
8. Press [PAGE DOWN].

## **RNX6x00/6150 Bridge/Router Configuration**

This section includes the following configuration procedures for the RNX6x00/6150 Bridge/Router:

- Configuring the RNX6x00/6150 Bridge/Router
- Configuring the RNX6300 Console

### **Configuring the RNX6x00/6150 Bridge/Router**

All MIB variables displayed using Config have a status of read/write. To set a single MIB variable in an RNX6x00 type bridge/router:

1. Choose LAN Control from the CMS 400 Commands menu.
2. Select RNX6x00 Bridge/Routers.
3. Enter the name of the RNX and press [PAGE DOWN].
4. Select Direct-SNMP.
5. Select Config. A variable list for the selected device is displayed.

6. Make the appropriate changes and press [PAGE DOWN].

## Configuring the RNX6300 Console

To configure the RNX6300 Console:

1. Choose LAN Control from the CMS 400 Commands menu.
2. Select RNX6300 User Console to display the VT220 window.

Log on to the system in the normal manner (refer to the *RACALAN NetExpress Operator's Guide*, Doc. No. LNX-8 for instructions).

3. After you have logged on, select Customize from the menu.
4. Select the first three items (System, Comm0, and Comm1) from the Activity window.
5. Select Modify from the Ring menu. The System Parameters screen is displayed first.

The information selected in the System Parameters screen should match the underscored selections displayed in the sample below.

6. Press [PAGE DOWN].
7. Press [SHIFT] - [ESC] to exit your RNX6300 Console screen and return to the CMS 400 screen.

RNX6300 Console On COM2:  
System Parameters

```

Date:                23/Apr/91
Time:                13:56:42
Modem:               Disable modem Enable modem
NMS port on:         No NMS comm0 comm1
Maximum number of alarms to save: 128
Network alarms collected: No Yes
Alarms are sent to:  Memory Disk
Delete oldest or newest alarms: Oldest Newest
Console time-out value: 30
Maximum number of old configuration files: 5
Node Identifier:     MCPnn (C2)
                    dd/mm/yy hh:mm:ss MCPnn
                    17 Alarms
System Parameters    Enter ^v <> PF4=Help PF1=Switch
Commit Default Undo Next Back Top
    
```

Press Shift-Escape To Cancel

The second screen displayed is the Comm Port 1 Customization Parameters, as illustrated below (the same parameters apply to Comm Port 0).

RNX6300 Console On COM2:  
Comm Port 1 Customization Parameters

Baud Rate for this port:           Autobaud 110 300 1200 2400 2400 4800  
                                  9600 19200

Number of data bits:               Eight Seven

Parity:                            None Odd Even Mark Space Autoparity

In-bound flow control:            Character modem De-assertion modem Assertion  
                                  No flow control

Out-bound flow control:          Character modem De-assertion modem Assertion  
                                  No flow control

In-bound start character:         11

In-bound stop character:         13

                                  17 Alarms   dd/mmm/yy hh:mm:ss MCPnn (C2)

Comm Port 1 Customization Parameters   Enter ^v <> PF4=Help PF1=Switch

Commit Default Undo Next Back Top

Press Shift-Escape To Cancel

In order to receive alarms from remote nodes within your network, those nodes must be included in your configuration. The LAN Internetworking System RNX Handler Definition file allows you to define those nodes and to redefine the severity levels of each alarm received from your RNX6300 Console.

# Chapter 4

## Monitoring SNMP Devices

---

### About This Chapter

This chapter describes the equipment-monitoring functions of the LAN Internetworking Manager. The following procedures describe how to:

- Monitor SNMP devices:
  - MIB variables
  - Front panel
  - Alarms
  - Statistics
- Monitor INX5000 chassis:
  - device front panel
  - Alarms
  - Ethernet buses
  - Token Ring CAUs
  - INX-10BT LINX FOIRL Statistics
- View the SNMP Top 16 Variables
- Examine the INX5000 Chassis
- Examine the INX T-Ring CAU
- Monitor an RNX6x00/6150 Bridge/Router
- Display RNX6x00/6150 Statistics
  - Traffic statistics
  - Maintenance statistics

### Monitoring SNMP Devices

This section describes how to monitor standalone SNMP devices, those that are not found with a chassis device. The procedures include displaying:

- MIB Variables
- Device front panel
- Device Alarms
- General Traffic Statistics

## Displaying MIB Variables

To display SNMP MIB object values on the screen, as a printed copy, or to save to a file:

1. Select the device type from the LAN Control menu.
2. Enter the name of the device and press [PAGE DOWN].
3. Select Direct-SNMP.
4. Select Fetch to display a list of all MIB categories.
5. Click on the MIB category to select it. A list of MIB objects is displayed. If there are more objects than will fit on a screen, press [PAGE DOWN] to see more.
6. Click on a MIB object to select it. (Click on the object a second time to unselect it.) Select as many objects as you like, and press [ESC] The MIB category screen reappears.
7. Press [ESC] again. The specific-instance prompt appears. If you want to display all the instances, leave the field blank. If you want to view for a specific instance, type the number in the field.
8. Press [PAGE DOWN] to display the Select A Destination menu. Choose one of the following output destinations:
  - None (return to the Unit Criteria Selection screen)
  - Screen
  - Hub Printer
  - Station Printer
  - Disk File
9. To select a destination, highlight your choice using the arrow keys, and press [PAGE DOWN].

## Displaying the Device Front Panel

To display the front panel of an SNMP device (except a device in a chassis):

1. Open the LAN Control Menu and select the "Control" option for the device type you want to display (e.g., INX T-Ring CAU Control).
2. Either type in the unit name, or make a selection from a pull-right menu by clicking on the pull-right menu symbol (>).
3. Press [PAGE DOWN].

## Displaying Alarms

To display SNMP-device alarms:

1. Open the LAN Control Menu and select the “Control” option for the device you want to display (e.g., INX T-Ring CAU Control).
2. Either type in the unit name, or make a selection from a pull-right menu by clicking on the pull-right menu symbol (>).
3. Press [PAGE DOWN].
4. Select Alarms from the screen legend.

## Displaying Statistics

To display the general transmit and receive statistics for an SNMP device:

1. Open the LAN Control Menu and select the “Control” option for the device you want to display (e.g., INX T-Ring CAU Control).
2. Either type in the unit name, or make a selection from a pull-right menu by clicking on the pull-right menu symbol (>).
3. Press [PAGE DOWN].
4. Select Stats from the screen legend.

## Monitoring INX5000 Devices

This section describes how to monitor SNMP devices located inside an INX5000 chassis. The procedures include displaying:

- The Device front panel
- Alarms
- Ethernet Buses
- Token Ring CAUs
- INX-10BT/INX-FOIRL Statistics

### Display a Device in the INX5000 Chassis

To display and access a device in the INX5000 chassis:

1. Select Generic SNMP Control from the LAN Control menu.

2. Locate the INX5000 chassis that you want to display. If the network has more devices than will fit on a single screen, press [PAGE DOWN] to see more devices.
3. Click on the specific INX5000 chassis.
4. Click on an INX5000 chassis device.

### **Displaying Alarms for an INX5000 Device**

To display alarms for a device in the INX5000 chassis:

1. Select Generic SNMP Control from the LAN Control menu.
2. Click on the INX5000 chassis.
3. Click on the INX5000 device.
4. Select Alarms.

### **Displaying Ethernet Buses in the INX5000**

To display Ethernet buses in the INX5000 chassis, follow these steps:

1. Select INX5000 Hub Control from the LAN Control menu.
2. Enter the name of the INX5000 Hub and press [Page Down].
3. Type [>] to view additional selections.
4. Select Buses to display the Internal Bus Configuration screen.
5. To view statistics for the Buses (see Table 4-1), select Statistics from the screen legend.

**Table 4-1. Internal Bus Statistics Screen Field Definitions**

<b>Field Name</b>	<b>Field Definition</b>
Frames Received	Number of frames detected.
Octets Received	Number of bytes associated with the frames detected.
Multicast Frames Received	Number of frames detected with an Ethernet multicast destination address.
Broadcast Frames Received	Number of frames detected with a broadcast destination address.
Normal Collisions	Number of collisions that occurred within 512-bit times of frame start. (These kinds of collisions are normal for networks with high utilization.)
Late Collisions	Number of collisions that occurred after 512-bit times of frame start.
CRC Errored Frames Received	Number of frames that are not fragments that have an illegal Ethernet frame-check sequence.
Collision Fragments Received	The number of collision fragments (frames less than 96 bits long) received on this bus.
Short Frames Received	Number of frames received on this bus that are between 8 and 63 octets long.
In-Range Errors Received	Number of in-range errors received on this bus. IEEE 802.3 frames contain a length field, indicating the length of the frame. If the value in the length field and the actual length of the frame do not match, the receiving device returns an in-range error.
Out-Range Errors Received	Number of out-range errors received on this bus. IEEE 802.3 frames contain a length field, indicating the length of the frame. If the length of the frame is outside of 802.3 parameters, the receiving device returns an out-of-range error.

**Table 4-1. Internal Bus Statistics Screen Field Definitions (Continued)**

<b>Field Name</b>	<b>Field Definition</b>
Too Long Errors Received	Number of frames received on this bus that are greater than 1520 octets long.
Non-aligned Frames Received	Number of frames received on this bus that are not an integral number of octets in length.
Missed Frames Received	Number of frames received while the INX-NMM receive state is disabled (usually because a network error condition has created a situation where resources are limited).
Bad Frames Received	Total number of frames received with CRC or alignment errors.

### **Display the INX T-Ring CAUs in the INX5000**

To display the INX T-Ring CAUs in an INX5000 chassis:

1. Select INX T-Ring CAU Control from the LAN Control menu.
2. Enter the name of any INX T-Ring CAU, and press [PAGE DOWN].
3. Select Chassis. The INX5000 chassis is displayed, along with which INX T-Ring CAU cards are located on which logical ring. The legend displays the following options:
  - Select Ring-Select to move a card in a slot to a bus.
  - Select Boot-Slot to boot to a specific card from within a slot.
  - Select Enable-Slot to enable a specific card within a slot.
  - Select Disable-Slot to disable a specific card within a slot.

### **Displaying INX-10BT, -MGR, FOIRL Statistics**

To display an INX-10BT, -MGR, and -FOIRL statistics on the INX5000 hub:

1. Choose LAN Control from the CMS 400 main menu.
2. Select INX Managed Repeater.
3. Either type in the unit name, or make a selection from a pull-right menu by clicking on the pull-right menu symbol (>).

4. Press [PAGE DOWN].
5. Select the module.
6. Select Stats.

The system displays the per-port statistics screen. Table 4-2 lists the field definitions for the Per-Port Statistics screen.

**Table 4-2. Per-Port Statistics Screen Field Definitions**

Field Name	Field Definition
State Of Port	If a port is disabled, no traffic can be transported to or from that port.
Frames Received	Number of frames received successfully off the bus by the SONIC. This value does not include frames received with FCS or alignment errors, or frames lost due to internal errors.
Octets Received	Number of octets associated with the frames included in the Frames Received field.
Multicast Frames	Number of frames received that have an Ethernet multicast destination address.
Broadcast Frames	Number of frames received that have an Ethernet broadcast destination address.
Normal Collisions	Number of collisions detected when the device attached to the port tried to transmit. Collisions occurred between 0 and 512 bit times after frame start (a normal collision for ports with high utilization).
CRC-Errored Frames	Number of frames received off this bus that are an integral number of octets in length (i.e., the number of bits they contain is a multiple of 8) and that do not pass the FCS check.
Short Frames	Number of frames received on this bus that are between 8 and 63 octets long.

**Table 4-2. Per-Port Statistics Screen Field Definitions (Continued)**

<b>Field Name</b>	<b>Field Definition</b>
In-Range Errors	Number of in-range errors received. If the value in the length field and the actual length of the frame do not match, the receiving device returns an in-range error.
Out-Range Errors	Number of out-range errors received on this bus. If the length of the frame is outside of 802.3 parameters, the receiving device returns an out-of-range error.
Last Source Address	Source address of the last frame successfully received.
Too Long Frames	Number of frames received that are greater than 1520 octets long, but not greater than 5 msec in duration (indicating a jabber condition).
Non-Aligned Frames	Number of frames received that are not an integral number of octets in length (i.e., the number of bits they contain is not a multiple of 8).
Autopartitions	Number of times that the port was automatically partitioned from the network because of an error detected by the INX-10BT or INX-FOIRL module. Autopartitions can be caused by a long collision (between 100 us and 3 ms), or by 31 consecutive short collisions (collisions less than 100 us that occurred less than 512 bit times after frame start).
TX Clock Violations	Number of times the device attached to the port transmits, but its frame cannot be decoded by the module because of a timing error. The timing error is usually caused by an error in the device's transmit logic.
Source Address Changes	Number of times that the Ethernet source address of a frame transmitted by the device attached to the port has changed from one frame to the next frame. If the port is attached to a bridge, this count will be very high.
Link Integrity Changes	Number of times that the device attached to the port has been disconnected. If no connection is found when the INX-10BT or INX-FOIRL module is rebooted, this counter increments by one.
Late Collisions	Number of collisions that occurred after 512 bit times of frame start.
MAU Jabber Lockups	Number of times that the port detects that the attached device is transmitting for more than 6 ms.

## Monitoring SNMP Top-16 Variables

The Top-16 feature allows you to select up to 16 MIB objects to monitor on a single, bar-graphed window. The variables can be any combination ranging from up to 16 MIB objects from a single device, to one MIB object for up to 16 devices. To monitor SNMP Top-16, follow these steps:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select SNMP Top-16 Monitor.

---

**Note:** If multiple objects are being viewed, the SNMP Monitor Bar Graph displays the monitored object name next to the bar graph.

---

The SNMP Top-16 Monitor screen allows you to specify up to 16 unit names. For each unit, select a MIB name, a MIB variable that returns a numeric value, and an instance number (zero if left blank). For each MIB variable, you can select lower and upper thresholds and indicate whether you want the bar graph to turn red if the number of elements returned by the MIB variables (for example, CRC errors) is within or beyond the lower and upper thresholds you specified.

You can also specify the number of seconds between polls, whether the bar graph represents the raw variable value or an integration per second, and whether CMS 400 skips a unit if it does not reply after a specified number of polls. You can set the scale of the bar graph to auto-range or to one of the 26 ranges offered by the system.

## Setting up the Top-16 Monitor

To set up unit types, MIB variables, thresholds, and other operating parameters that you want represented on the bar graph:

1. Select SNMP Top-16 Monitor from the LAN Control menu.
2. Select Setup. A screen similar to Figure 4-1 is displayed.



1. Choose LAN Control from the CMS 400 main menu.
2. Select Generic SNMP Control.
3. Click on the INX5000 icon.

The system displays a front view of the INX5000 Chassis.

4. Click on the device. This displays a graphic of the device.
5. Select Monitor from the screen legend. The Reporting Options screen (Figure 4-3) is displayed.

Reporting Options	
Source Of Display Data	Poll Unit
Analysis Of Display Data	Raw Counts
Initial Display Format	Text
If Polled From Unit:	
Specific Instance	
Duration Of Monitoring	Seconds
Interval Between Polls	1 Seconds
File To Store Values In	.MON
If Retrieved From File:	
File To Fetch Values From	.MON

**Figure 4-3. Reporting Options Screen**

6. Specify the source of the display data (poll unit or read file), how you want the data to appear (text, bar chart, or graph plot), the file name (if you choose to read a file), and how you want data polled (if you choose to poll the unit).
7. Press [ENTER] to move from field to field.

Table 4-3 lists the field definitions for the Reporting Options screen.

**Table 4-3. Reporting Option Screen Field Definitions**

<b>Field Name</b>	<b>Field Definition</b>
Source of Display Data	Indicates whether you want the data to come from the selected unit, or fetched from a *.MON file. Valid selections are Poll Unit or Read File. Press [TAB] until the selection you want appears in the field.
Analysis of Display Data	Indicates whether you want the data to be displayed as raw counts or per second rates. Press [TAB] until the selection you want appears in the field.
Initial Display Format	Indicates whether the results are displayed as text, bar chart (bar graph), or graph plot (plotted points). You can change the display format later, while the system displays the results.
Specific Instance	If you selected Poll Unit in the Source of Display data field, enter the MIB object instance (null for first).
Duration of Monitoring	If you selected Poll Unit in the Source of Display data field, enter the number of seconds, minutes, hours, or days you want to monitor a specific variable for the device.
Interval Between Polls	If you selected Poll Unit in the Source of Display data field, enter the number of seconds, minutes, hours, or days between polls.
File To Store Values In	If you selected Poll Unit in the Source of Display data field, enter the name of the *.MON file in which you want to store the data results. This field is optional.
File To Fetch Values From	If you selected Read File in the Source of Display data field, enter the name of the file from which you want to retrieve the data values.

8. When you have completed the Reporting Options screen, press [Page Down] to accept the input. The select a MIB screen is displayed.
9. Use the arrow keys to select a MIB. A Select Variable screen similar to Figure 4-4 is displayed.

Select Only A Single Object As Defined In MIB MIB2	
System Up Time	Interface Tx Characters
System Services	Interface Tx Unicast Packets
Number Of Interfaces	Interface Tx Multicast Packets
Interface Index	Interface Tx Packets Discarded
Interface Type	Interface Tx Packets With Errors
Interface Largest Datagram	Interface Tx Queue Size
Interface Speed	AT Table Interface Index
Interface Desired State	IP Forwarding Status
Interface Current State	IP Default Time To Live
Interface Last Change Uptime	IP Rx Datagrams Total
Interface Rx Characters	IP Rx Datagrams Header Errors
Interface Rx Unicast Packets	IP Rx Datagrams Address Errors
Interface Rx Multicast Packets	IP Datagrams Forwarded
Interface Rx Packets Discarded	IP Rx With Unknown Protocol
Interface Rx Packets With Errors	IP Rx Datagrams Discarded
Interface Rx Unknown Protocol	IP Rx Datagrams Delivered

ESC: Done PgDn/PgUp: Pages Home/End: MIBs Tab: Mark Spa: Unmark Zoom Alias

**Figure 4-4. Select Variable Screen**

10. To select a variable to monitor, press [ENTER] until the cursor is next to the MIB variable you want to view.
11. Press [TAB] to mark the variable.
12. Press [ESC] to display the data.

Table 4-4 describes the function keys for the Select Variable screen.

**Table 4-4. Select Variable Function Keys**

<b>Key</b>	<b>Description</b>
[ESC]	Displays the screen shown in Figure 3-3.
[PAGE DOWN] or [PAGE UP]	Displays the list of MIB variables in the selected device, one page at a time.
[HOME] or [END]	[HOME] displays the beginning of the list of MIB II variables. [END] displays the beginning of the list of private extensions. (Device specific MIBs.)
[TAB]	Selects the variable.
[SPACE]	Unselects the variable (Fetch function only).
[ZOOM]	Displays specific information for the selected variable.
[ALIAS]	Toggles between the object descriptors and the aliases.

## Examining the INX5000 Chassis

To examine the INX5000 chassis:

1. Choose INX5000 Hub Control from the LAN Control menu.
2. Enter the name of the INX5000 and press [PAGE DOWN].

The system polls the INX-NMM or INX-MGR for the chassis configuration and displays the front view of the INX5000 chassis.

3. Select Examine. A screen showing the current status of the selected module is displayed. Also, the configuration parameters for the selected module can be displayed and modified.

You can view the module's hardware, software, and firmware revisions by moving the module from one bus to the other; and enabling, disabling or rebooting the module.

Table 4-5 lists the field definitions for the Examine Module Screen.

**Table 4-5. Examine Module Screen Field Definitions**

<b>Field Name</b>	<b>Field Definition</b>
Slot and Unit	Slot number of the slot in which the module is installed, and the type of module installed in that slot.
Logic Module	Logic module component of the module.
Status	Allows you to enable, disable, or reboot the module.
Serial Number	Serial number of the logic module component.
Internal NIC Bus	Ethernet bus in the chassis (A or B) to which you want the module connected. If you want to connect a module to Bus B, an INX-NMM or INX4000/L paired with a backbone connectivity module must be installed in the chassis, and the backbone connectivity module must be configured to run on Bus B.
Temp	Indicates whether the chassis temperature is OK.
Hardware Rev	Hardware revision level of the logic module component of the module.
Software Rev	Revision level of the CMP image currently running on the module.
Firmware Rev	Level of the module's firmware.
IP Address	Internet address for the module.
Connectivity Module	The connectivity module component of the module.
Status	Allows you to disable or enable the connectivity module.
Serial Number	Serial number of the connectivity module connected to the logic module.
Internal Bus	Ethernet bus in the chassis (A or B) on which the backbone connectivity module paired with the INX-NMM or INX4000/L is enabled.

**Table 4-5. Examine Module Screen Field Definitions** (Continued)

Field Name	Field Definition
Media	The media type you want to use to connect the backbone connectivity module to the backbone network. Press [TAB] to toggle between Thin/fiber (ThinNet/Fiber-Optic port) and Thick (AUI port). This field applies to the INX-NMM and the INX4000/L.
Sonic Bus	Ethernet bus in the chassis (A or B) for which you want the INX-NMM to monitor bus summary, INX-FOIRL, and INX-10BT statistics. This choice can be different from the Internal Bus selection.
Hardware Rev	Hardware revision level of the connectivity module component of the module.

## Examining the INX T-Ring CAU

To examine the INX T-Ring CAU:

1. Select INX T-Ring CAU Control from the LAN Control menu.
2. Enter the name of the INX T-Ring CAU and press [PAGE DOWN].  
A screen showing the current status of the selected module is displayed.

You can view the module's hardware, software, and firmware revisions, and enable, disable, or reboot the module.

## Monitoring an RNX6x00/6150 Bridge/Router

This procedure dynamically polls the current unit for a single MIB variable value, or replays a monitor session previously recorded to a \*.MON file. This procedure does not apply to RNX6300s.

1. Select RNX6x00 Bridge/Routers from the LAN Control menu.
2. Enter the name of the RNX and press [PAGE DOWN].
3. Select Monitor. The Reporting Options screen is displayed.

Reporting Options	
Source Of Display Data	<b>Poll Unit</b>
Analysis Of Display Data	Raw Counts
Initial Display Format	Text
If Polled From Unit: Specific Instance	
Duration Of Monitoring	Seconds
Interval Between Polls	1 Seconds
File To Store Values In	.MON
If Retrieved From File: File To Fetch Values From	.MON

**Figure 4-5. Reporting Options Screen**

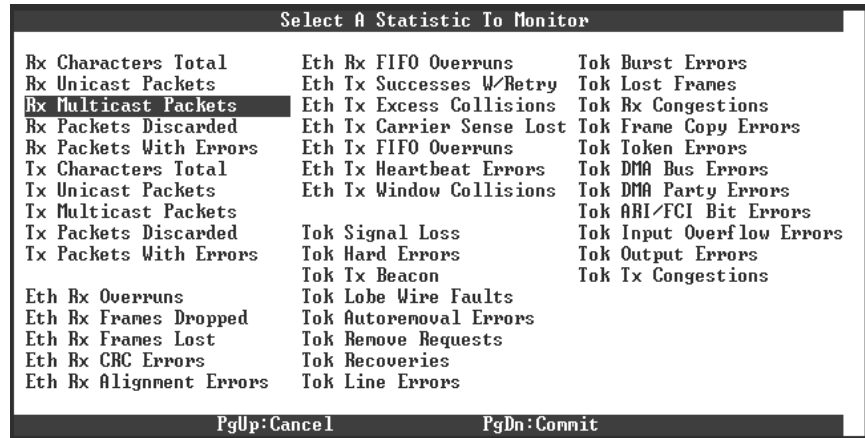
**Note:** The field Specific Card to Poll appears in place of the field Specific Instance for the RNX6x00. This field is used if you selected Poll Unit in the Source of Display data field.

4. Specify the source of the display data (poll unit or read file), how you want the data to appear (text, bar chart, or graph plot), the file name (if you choose to read a file), and how you want data polled (if you choose to poll the unit).
5. Press [ENTER] to move from field to field. Table 4-6 lists the field definitions for the Reporting Options screen.

**Table 4-6. Reporting Option Screen Field Definitions**

<b>Field Name</b>	<b>Field Definition</b>
Source of Display Data	Indicates whether you want the data to come from the selected unit, or fetched from a *.MON file. Valid selections are Poll Unit or Read File. Press [TAB] until the selection you want appears in the field.
Analysis of Display Data	Indicates whether you want the data to be displayed as raw counts or per second rates. Press [TAB] until the selection you want appears in the field.
Initial Display Format	Indicates whether the results are displayed as text, bar chart (bar graph), or graph plot (plotted points). You can change the display format later, while the system displays the results.
Specific Instance to Poll/Specific Card to Poll	If you selected Poll Unit in the Source of Display data field, enter the MIB object instance (null for first).
Duration of Monitoring	If you selected Poll Unit in the Source of Display data field, enter the number of seconds, minutes, hours, or days that you want to monitor a specific variable for the device.
Interval Between Polls	If you selected Poll Unit in the Source of Display data field, enter the number of seconds, minutes, hours, or days between polls.
File To Store Values In	If you selected Poll Unit in the Source of Display data field, enter the name of the .MON file in which you want to store the data results. This field is optional.
File To Fetch Values From	If you selected Read File in the Source of Display data field, enter the name of the file from which you want to retrieve the data values.

6. Press [PAGE DOWN] to accept the input. A Select Statistic screen similar to Figure 4-7 is displayed.



**Figure 4-7. Select Statistic Screen**

7. Press [ENTER] to display the data in the format you selected in the Initial Display Format field.

## Displaying RNX6x00/6150 Statistics

The following procedures describe how to view RNX6x00/6150 bridge/router statistics. There are procedures for displaying:

- Traffic statistics
- Maintenance statistics

### Displaying Traffic Statistics

To display the traffic statistics for each module in the RNX6x00 bridge/router:

1. Select RNX6x00 Bridge/Routers from the LAN Control menu.
2. Enter the name of the RNX and press [PAGE DOWN].
3. Select Stats. The traffic statistics for each module in the RNX6x00/6150 type bridge/router are displayed.

## Displaying Maintenance Statistics

To display maintenance-related statistics for a selected module in the RNX6x00/6150 bridge/router:

1. Select RNX6x00 Bridge/Routers from the LAN Control menu.
2. Enter the name of the RNX and press [PAGE DOWN].
3. Select the module in the RNX.

If the module has its own SNMP agent, you can fetch and display a number of maintenance-related statistics from a selected module in the RNX bridge/router.

# Chapter 5

## Control Operations

---

### About Control Operations

The CMS 400 provides the capability to perform various network control operations on one or multiple LAN internetworking devices.

This chapter includes the following procedures:

- Reading/Writing SNMP MIB Variables
- Opening and Rotating the INX5000 Chassis
- Reinitializing an SNMP Device
- Pinging an SNMP Device
- Disabling and Enabling an SNMP Device
- Rebooting an SNMP Device
- Accessing Telnet from INX T-Ring CAU Control
- Opening and Closing the RNX6x00/6150 Panel
- Accessing the Cut-Through to the RNX6300 Console
- Directing SNMP GET/SET Control
- Displaying MIB Objects in a Unit
- Accessing Telnet from Generic SNMP Control
- Accessing Telnet from an RNX6x00/6150

### Reading/Writing SNMP MIB Variables

This procedure lets you read several variables from a selected SNMP unit. To display the values returned by the MIB variables:

1. From the LAN Control menu, select the device type (e.g. INX5000 Hub Control).
2. Enter the name of the device, and press [PAGE DOWN].
3. Select Direct-SNMP values for a specific module.
4. Select Fetch to bring up the MIB selection screen.
5. Select a MIB and press [ENTER]. A list of all variables for which you can view returned values is displayed.

6. Press [TAB] to select the variable. The system places a red checkmark next to the variable.
7. After you have finished selecting variables, press [ESC]. The MIB screen is displayed.

**To Read a MIB file:**

- a. Select Read-File. You are prompted to enter the name of the object.
- b. Press [TAB] to scroll to the object you want to select, and press [PAGE DOWN]. The selected variables are read.

**To Write a MIB file:**

- a. Select Write-File. You are prompted to enter the name of the object.
  - b. Press [TAB] to scroll to the object you want to select and press [PAGE DOWN]. The selected variables are written to a file.
8. Press [ESC] again. The specific instance of this MIB variable prompt is displayed. If you know what your specific instance is, type it in the prompt. If you want to display all the instances, leave the prompt blank.
  9. Press [PAGE DOWN].
  10. Select one of the following destinations for the report:
    - None (Previous Page)
    - Screen
    - Hub Printer
    - Station Printer
    - Disk File
  11. Press [ENTER].

## Opening and Rotating the INX5000 Chassis

To open and rotate an INX5000 chassis:

1. Select INX5000 Hub Control from the LAN Control menu.
2. Enter the name of the INX5000, and press [PAGE DOWN].
3. Select Open. A graphic representation of the INX5000 front panel opens so that you can see the modules that are installed.
4. Select Rotate to view the modules from the rear of the chassis.

To redisplay the front of the chassis, select Rotate again.

## Reinitializing an SNMP Device

To reinitialize a device and load its operating software:

1. From the LAN Control menu, select the device type (e.g. INX5000 Hub Control).
2. Enter the name of the device, and press [PAGE DOWN].
3. Type [>] to view additional selections.
4. Select Reboot. The system reinitializes the module and, if applicable, reloads the module's operating software image.

## Pinging an SNMP Device

To ping an SNMP device that is not inside a chassis:

1. Open the LAN Control Menu and select the "Control" option for the device type you want to display (e.g., INX T-Ring CAU Control).
2. Either type in the unit name, or make a selection from a pull-right menu by clicking on the pull-right menu symbol (>).
3. Press [PAGE DOWN].
4. Select Ping from the screen legend.

The system reports whether the ping was successful or not.

## Disabling and Enabling an SNMP Device

To disable or enable a single port on a suitable SNMP device

1. Open the LAN Control Menu and select the control option for the device type you want to display (e.g., INX T-Ring CAU Control).
2. Either type in the unit name, or make a selection from a pull-right menu by clicking on the pull-right menu symbol (>).
3. Press [PAGE DOWN].
4. Select the port.
5. Select On/Off. The port is disabled or enabled, depending on the original state of the port. A graphic indicator similar to the actual hardware indicates the port's status.

## Rebooting an SNMP Device

To reboot an SNMP device:

1. Open the LAN Control Menu and select the control option for the device type (e.g., INX T-Ring CAU Control).
2. Either type in the unit name, or make a selection from a pull-right menu by clicking on the pull-right menu symbol (>).
3. Press [PAGE DOWN].
4. Type [>] or click on the > at the far right of the screen legend.
5. Select Boot. The following prompt is displayed: Are You Certain? Press Y to Confirm, Any Other to Cancel.
6. Press **Y** to boot the device.

## Accessing Telnet from INX T-Ring CAU

To access Telnet from the INX T-Ring CAU control:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select INX T-Ring CAU Control from the LAN Control menu.
3. Enter the name of the INX T-Ring CAU that you want to access, and press [PAGE DOWN].
4. Select Telnet. You can now access devices on the LAN that support the Telnet Network Virtual Terminal (NVT) protocol.

Telnet displays a VT type terminal emulator for the INX T-Ring CAU. Refer to the individual product guides for additional information about how to use Telnet.

**Note:** Only one Telnet session at a time is supported.

5. You can specify a unit name, from the database, on an explicit IP address. Additionally, the port number may be specified in place of the well-known Telnet port number, which is 23. Once the session is established with the device, the session may be exited by pressing [SHIFT] - [ESC].

## Opening and Closing the RNX6x00 Panel

This procedure explains how to open and close the graphic front panel on the RNX6x00 so that you can view the modules installed in the device.

1. Select RNX6x00 Bridge/Routers from the LAN Control menu.
2. Enter the name of the RNX6x00 that you want to access, and press [PAGE DOWN].
3. Select Open. The modules in the RNX6x00 graphic are displayed. You can now select a module in the router.
4. To close the front panel on a RNX6x00, select Close.

## Accessing the Cut-Through to the RNX6300 Console

To access the cut-through to the RNX6300 Console:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select RNX6300 User Console. The VT220 emulation window to the device is displayed.

## Directing SNMP GET/SET Control

This procedure allows you to invoke the SNMP Control function. To offer direct SNMP GET/SET control:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select Define SNMP Applications from the LAN Control menu.
3. Choose Direct SNMP.
4. Enter the unit information and press [PAGE DOWN].

The SNMP Control function is invoked so you can access SNMP GET/SET control.

## Displaying MIB Objects in a Unit

To display every MIB object for a selected unit:

1. Choose LAN Control from the CMS 400 Main menu.
2. Select Generic SNMP Control. The generic SNMP control screen is displayed.
3. Select a device icon.
4. Select Dump.

5. Type a dump variable and use the arrow keys to highlight the interval between each retrieve.
6. Select either None, 0.5 sec, or 1 sec delay for displaying your received unit variables.
7. Press [PAGE DOWN] to allow the unit-variables to be displayed. The system gets and displays every MIB object for the selected unit.

Press the space bar to pause the unit-variables display.

or

Press [ESC] to cancel the unit-variables display.

## Accessing Telnet from Generic SNMP Control

To access Telnet from the Generic SNMP Control:

1. Select Generic SNMP Control from the LAN Control menu.
2. Select a unit icon.
3. Select Telnet. You can access devices on the LAN that support the Telnet Network Virtual Terminal (NVT) protocol.

Telnet displays a VT type terminal emulator for devices on the LAN that support Telnet, such as the INX5000 NMM, and NTS products. Refer to the individual product guides for additional information about how to use Telnet.

---

**Note:** Only one Telnet session at a time is supported.

---

4. You can specify a unit name from the database, on an explicit IP address. Additionally, the port number may be specified in place of the well known Telnet port number, which is 23. Once the session is established with the device, the session may be exited by pressing [SHIFT] - [ESC].

## Accessing Telnet from an RNX6x00

To access Telnet from the a RNX6x00:

1. Select RNX6x00 Bridge/Routers from the LAN Control menu.
2. Select a unit type and press [PAGE DOWN].

3. Select Telnet. You can now access devices on the LAN that support the Telnet Network Virtual Terminal (NVT) protocol. This implementation of NVT is simple, with minimal negotiated options.

Telnet displays a VT type terminal emulator for devices on the LAN that support Telnet, such as the RNX6x00 type bridge/router products. Refer to the individual product guides for additional information about how to use Telnet.

---

**Note:** Only one Telnet session at a time is supported.

---

4. You can specify a unit name from the database, at an explicit IP address. Additionally, the port number may be specified in place of the well known Telnet port number, which is 23. Once the session is established with the device, the session may be exited by pressing [SHIFT] - [ESC].



# Appendix A

## Network Interface Card Types

---

### Description

These are the possible Network Interface Card types that are certified to be compatible with the CMS 400 in a hub platform:

3COM 3C503

3COM 3C505

3COM 3C523

Milgo Etherblaster

Milgo MCA

Milgo NI3210

Western Digital Ethercard Plus

IBM 4/16 Token Ring adapter (ISR and MC)

3COM 4/16 Token Ring adapter (ISA and MC)

Milgo ISA and MC Token Ring Adapters



# Appendix B

## Custom SNMP Applications: A Tutorial

---

### Introduction

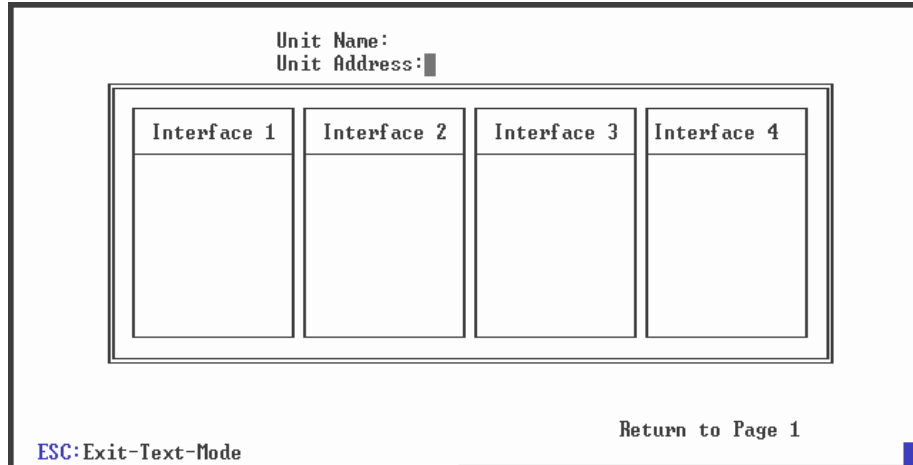
You can create your own SNMP monitoring applications with CMS 400's Custom SNMP Application. This tutorial walks you step-by-step through the creation of a sample application.

### The Tutorial Application

Typically, before you create an application, you need to design it. The tutorial application is designed to monitor up to four interfaces on a device. It also provides basic information about the device, and provides some links to related screens. This application takes up two application "pages." The final application pages will look like Figures B-1 and B-2.

Test Application		Action Menu:
Unit Name: UNIT_00091		-----
IP Address: 130.45.71.254		Go to Device Icon
Unit Type: RNX6500 Router	Alarms in	Go to Display Alarms
Site Name:	Queue?	Monitor Card #1
Location: CMS400_LAB		Monitor Card #2
Number of Interfaces: 4		-----
Interface 1	Interface 2	
Type: Ethernet/802.3	Type: ProNET-4/16	
Desired State: up(1)	Desired State: up(1)	
Current State: up(1)	Current State: up(1)	
Characters TX: 76862353	Characters TX: 40069375	
Interface 3	Interface 4	
Type: Dual Serial Line	Type: Dual Serial Line	
Desired State: up(1)	Desired State: up(1)	
Current State: down(2)	Current State: down(2)	
Characters TX: 0	Characters TX: 0	

Figure B-1. Test Application, Page One



**Figure B-2. Test Application, Page Two**

Page one features general data about the unit. Page two is a “phantom” page with no real application data, but it demonstrates the graphic tools available in the Custom SNMP application.

## Collect Data on the Target Device

Before you start, it's a good idea to have a specific target device to run your application on. Since this sample application will monitor up to four network interfaces, select a unit on your network that has multiple interface devices to monitor. The target unit in the samples is an RNX6500 router.

### Fetch MIB Values

First, use Fetch to collect the data that will be incorporated into the application:

1. Select Generic SNMP from the LAN Control menu.
2. Click on the target device's icon.
3. Select Fetch from the screen legend.
4. Select MIB2 from the listing of MIB files.
5. Choose the following MIB Objects:

System Description

Number of Interfaces

Interface Type

Interface Desired State

Interface Current State

Interface Tx Characters

6. Press [ESC] twice.
7. Press [PAGE DOWN] at the Instances window, leaving it blank. You will see a screen similar to Figure B-3.

```

Unit Variables Received
System Description.0      Portable AMD29000 C Gateway 16THUB5 S/N 14545
                          U13.0dl1
Number Of Interfaces.0   4
Interface Type.1         ethernet-csnacl<6>
Interface Type.2         iso88025-tokenRing<9>
Interface Type.3         propPointToPointSerial<22>
Interface Type.4         propPointToPointSerial<22>
Interface Desired State.1 up<1>
Interface Desired State.2 up<1>
Interface Desired State.3 up<1>
Interface Desired State.4 up<1>
Interface Current State.1 up<1>
Interface Current State.2 up<1>
Interface Current State.3 down<2>
Interface Current State.4 down<2>
Interface Rx Characters.1 370862008

ESC:Cancel      PgDn:Next Page      Home:Restart      Refetch
Please Press Any Key To Continue ...
    
```

**Figure B-3. MIB Variables Received Screen**

Make a note of the information (for the first four interfaces). It may be useful when you set up your application. Use the chart below.

IF #	Type	Des. State	Current State	RX	TX
1					
2					
3					
4					

## Setting General Application Parameters

You can now start building your application. This involves:

- Creating an application file

Setting the refresh rate of the application screen

Setting the general system parameters

### Creating the Application File

To create the application file:

1. Select Define SNMP Application from the Application menu.
2. Double-click on the Add Application selection. A window appears, prompting you to type in a file name for the application. (The first character is filled in with a dollar sign; this character cannot be changed.)
3. Type: **testapp** [ENTER]. The application name will be \$TESTAPP. (You can enter any name up to seven characters long.)
4. A new application screen appears with an introductory message. You're ready to go on to the next procedure.

### Setting the Refresh Rate

This operation sets the rate at which the application screen is updated with new data. You will set the refresh rate to every three seconds. Follow these steps:

1. Select Setup from the screen legend. A Screen Update, text-entry window appears.
2. Type: **3** [ENTER].
3. Press [PAGE DOWN] to accept the input and return to the new application.

### Setting the General Parameters

To set some general parameters for the application, follow these steps:

1. Select General from the screen legend.
2. Enter a Long Application Name (e.g. Test Application 1).
3. Enter a Short Application Name (usually the file name).
4. Accept the default Target Unit Selection field. It should read Prompt for One Unit. If it does not, click on the field and press [TAB] until it appears.
5. Press [PAGE DOWN]. The Selectable SNMP Variables for the Monitor Subfunction window appears.

6. Press [PAGE DOWN] to accept the MIB2 default. The Selectable SNMP Variables for the Configure Subfunction window appears.
7. Press [PAGE DOWN] to accept the MIB2 default and return to the application screen.

You're now ready to create the first page of the application screen.

## Setting up the First Application Page

Setting up the first page of the application involves choosing the background color of the screen, choosing the color of the text, and entering the background text.

### Specifying the Colors

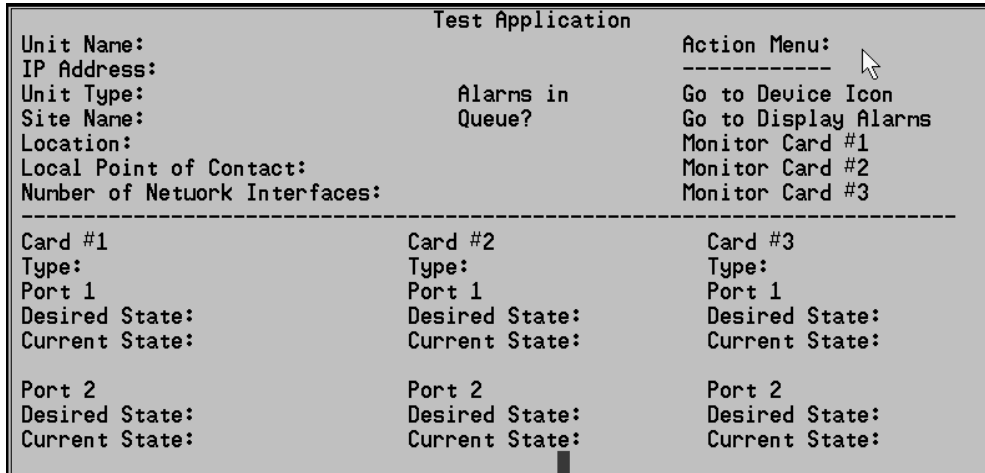
To specify the colors for the text and the screen's background, follow these steps from the first page of the new application:

1. Select Backdrop from the screen legend. The backdrop screen appears.
2. Select Colors from the screen legend. A window appears, indicating color default as White on Black.
3. Change the color scheme to Black on White. Click on the field and press [TAB] until the required color appears.
4. Press [PAGE DOWN] to accept the new color scheme and to return to the Backdrop screen.
5. Select Flood from the screen legend. The background screen will change to the selected colors. You're ready to go on to the next procedure.

### Adding Background Text

In this step you will add the text to the background screen. Follow these steps from the background screen:

1. Select Text-Mode from the screen legend.
2. Enter the text as shown in Figure B-4. You can position the cursor by clicking on the screen location. You can delete the previous character by pressing [BACKSPACE], and you can overwrite an existing character. You cannot, however, delete a character with the [DELETE] key.



**Figure B-4. Page One Background**

3. Press [ESC] to exit Text-Mode.
4. Press [ESC] to exit Backdrop Mode.
5. Type **Y** to save the changes.
6. Press [ESC] to back out of the application and ensure saving your work.

## Adding MIB Variable Fields

In this section, you will select and place the MIB variable fields onto the background screen. There are two slightly different procedures in this section:

Adding Name, Address, and Type Fields

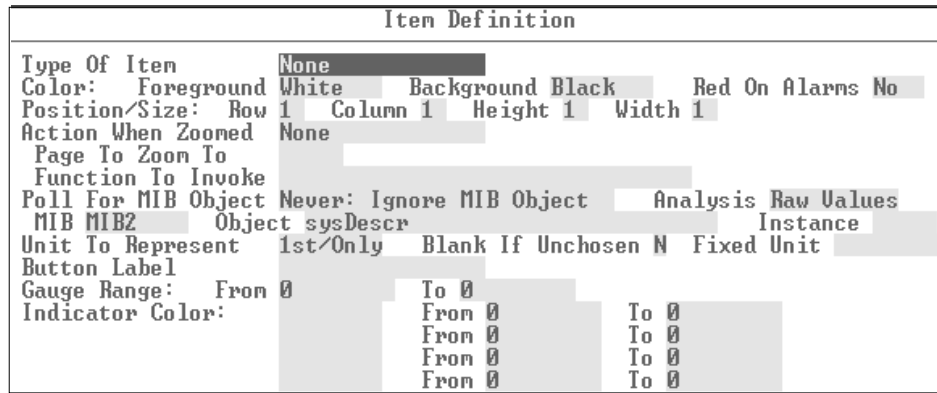
Adding MIB2 Variable fields

### Adding Name, Address, and Type Fields

In this procedure, you will add the variable fields for the Unit Name, IP Address, Unit Type, and the Site Name:

1. Select Define SNMP Application from the Applications menu.
2. Select Modify Application.
3. In the Application Name field, press [TAB] until the name of your application appears.
4. Press [PAGE DOWN].

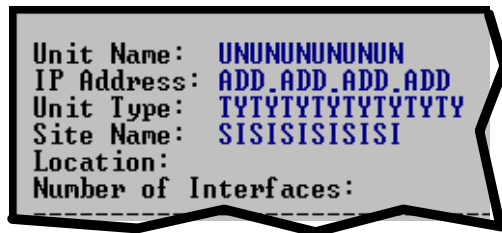
5. Select Items from the screen legend.
6. Select Add-Item from the screen legend. You will see the Item Definition screen.



**Figure B-5. Item Definition Screen**

7. Click on the Type Of Item field and press [TAB] until Unit Name appears.
8. Change the Foreground field to Red and the Background field to White.
9. Press [PAGE DOWN], (leave all other fields at the default values).
10. At the application screen, in the upper left corner, you will see the Unit Name field as the character string UNUNUNUNUN.
11. Select Position-Item from the screen legend.
12. Click on the space that is about two characters to the right of the Unit Name field label. The field moves to this position.

Repeat this procedure for the IP Address, the Long Unit Type, and the Site Name. When you're finished, the upper left corner of the screen should look like Figure B-6.



**Figure B-6. Current Fields**

### **Adding Single MIB2 Variables**

In this procedure, you will add the single MIB2 object variables: the Location and the Number of Interfaces. You should still be at the Items screen.

1. Select Add-Item from the screen legend. You will see the Item Definition screen.
2. Fill out the Item Definition screen as follows:  
  
Type of Item: MIB Object Value  
  
Colors: Red on White  
  
Poll for MIB Object: When page is first painted  
  
Object: sysLocation
3. Press [PAGE DOWN] (leave all other fields at the default values).
4. At the application screen, in the upper left corner, you will see the Unit Name field as the character string VAVAVAVAVAVA.
5. Select Position-Item from the screen legend.
6. Click on the space two characters to the right of the field label. The field moves to this position.

Repeat this procedure, but this time, in Step 2, at the Object field, select ifNumber. Position this variable next to the Number of Interfaces label.

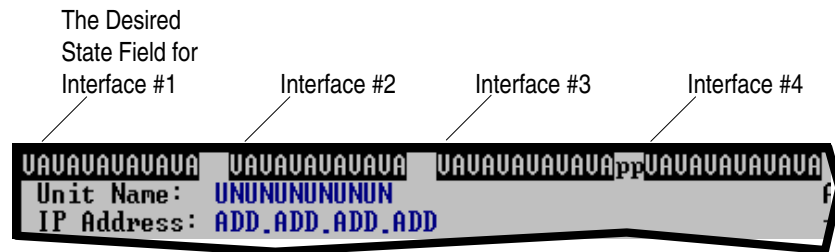
### **Adding Multiple Variables**

In this procedure you will add the MIB2 object variables for the three interfaces: the Desired State, current State, and Characters TX. You should still be at the Items screen.

1. Select Add-Item from the screen legend.
2. Fill out the Item Definition screen as follows:  
  
Type of Item: Mib Object Value  
  
Colors: Red on White  
  
Poll for MIB Object: At Every Screen Update  
  
Object: ifAdminStatus (the desired state)

**Note:** A handy way to enter the object field variable is to click on the field, type in the first several characters of the variable, and end with an asterisk (\*). For example, to enter ifAdminStatus, type in ifA\*, and press [ENTER]. If the field you want doesn't appear, you'll just need to press [TAB] until you reach the desired value.

3. Press [PAGE DOWN] (leave all other fields at the default values).
4. At the application screen, in the upper left hand corner, you will see the Unit Name field as the character string VAVAVAVAVA.
5. Select Replicate-Item from the screen legend. A field entry box appears.
6. Accept the default of the From value (1). Change the To value to 4. (You can do this by pressing [SHIFT] - [TAB] to count down.)
7. Leave the Arranged field to Horizontally, but change the offset to 14.
8. Press [PAGE DOWN]. You will see four Desired State variable fields at the top of your screen (Figure B-7).



**Figure B-7. Replicated Fields**

9. Click on the first character of the variable field for Interface Number 1.
10. Select Position-Item from the screen legend.
11. Click on the space two characters to the right of the field label. The field moves to this position. Position the other three variables.

Repeat this procedure for the Current State fields (ifOperStatus), and the Characters TX fields (ifOutOctets).

## Checking Your Progress

Now that you've entered all the variable fields, this will be a good time to check your progress and run the application.

1. Press [ESC] twice to close out of the application. You should be at the Define SNMP Application popup window.

2. Double-click on Test Application. An application name field appears.
3. If the name of your tutorial application is not already in the Application Name field, press [TAB] repeatedly until it appears.
4. Press [PAGE DOWN]. The unit name entry window appears.
5. Enter the selection criteria for the target unit and press [PAGE DOWN].

Your application should be running. The fields should display the proper information. Also, every few seconds, the Characters TX fields will be updated.

To get back to the Define Application menu:

1. Press [ESC] to exit the application.
2. Press [PAGE UP] to return to the Define Application selection menu.

You are ready to move on to the next section.

## Adding Alarm Handling

The alarm handling function of the tutorial application includes an indicator LED that turns red when there is an alarm in the queue, and an action menu selection that will jump to the device's Display Alarm screen. The first procedure will add the LED, and the second will create the jump to the Display Alarm screen.

### Adding the Alarm Indicator

To add the Alarms in Queue indicator, follow these steps from the Modify Application screen:

1. Select Items from the screen legend.
2. Select Add-Item.
3. Fill in the Item Definition screen as follows:

Type of Item: Round LED

Red on Alarms: Both

Leave all other fields at their default values.

4. Press [PAGE DOWN]. The new item will appear in the upper left corner.
5. Select Position-Item from the screen legend.

6. Click on the space under the “n” in the text Alarms in Queue? The LED will move to that position.
7. Press [ESC].

### Adding the “Go to Alarms” Item

To add the item that will take you to the unit’s alarm display, follow these steps from the Items screen:

1. Select Add-Item.
2. Fill in the Item Definition screen as follows:  
Type of Item: Invisible Button  
Width: 20  
Action When Zoomed: Invoke Function  
Function to Invoke: (type in) **DIS\_ALA UNI=%UN1**

---

**Note:** Be careful to type **UNI** (uppercase I) = **%UN1** (numeral 1).

---

Leave all other fields at their default values.

3. Press [PAGE DOWN]. The new item will appear in the upper left corner.
4. Select Position-Item from the screen legend.
5. Click on the “G” in Go to Display Alarms text.
6. Press [ESC].

### Adding the Link to Page 2

This procedure lays the groundwork for developing the second page of the application. To add the Zoom-to-Page item to Page 1:

1. Select Add-Item.
2. Fill in the Item Definition screen as follows:  
Type of Item: Invisible Button  
Width: 20

Action When Zoomed: Zoom to Page

Page to Zoom To: 2

Leave all other fields at their default values.

3. Press [PAGE DOWN]. The new item will appear in the upper left corner.
4. Select Position-Item from the screen legend.
5. Click on the "G" in Go to Device Icon text.
6. Press [ESC].

That's all the work you'll be doing on Page 1. The next phase of the operation involves using the Define Applications drawing tools to create page 2 of our sample application.

This would be a good time to test your application. If you have a suitable unit with alarms in the queue, run your application for it and test your link to the alarms display.

## Developing Page 2

The second page of the tutorial demonstrates the drawing tools in the Custom SNMP Application tool. It also demonstrates the way to create links between pages in the application. The procedures in this section include:

Creating the Page and Links

Drawing the Background

### Creating the Page and Links

The first step involves creating the new page, and providing a link back to page 1 of the application. Follow these steps from page 1 of the application:

1. Select Add from the screen legend. This opens a new Page 2 for the application.
2. Select Backdrop. Change the color scheme from White on Black to Black on White, remember to use Flood to repaint the backdrop.
3. Select Text-Mode from the screen legend. At the bottom right corner of the screen enter the text: Return to Page One.
4. Press [ESC] to exit Text-Mode.
5. Type **Y**, to confirm the changes.

6. Create a new item as follows:

Type of Item: Invisible Button

Width: 20

Function When Zoomed: Zoom to Page

Page to Zoom: Page 1

Leave all other fields at their defaults.

7. Position the invisible button over the Return to Page One text.

8. Test the link to make sure it works.

## Creating the Background

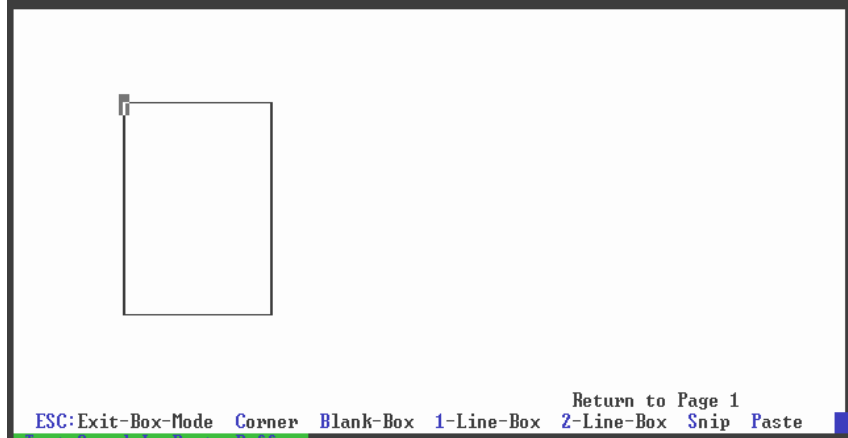
This lesson focuses on the drawing tools of the Custom Application Utility. The tool allows you to draw basic boxes and lines, and do some cutting and pasting. The final Page 2 will look like Figure B-8.

Unit Name:		Unit Address: █	
Interface 1	Interface 2	Interface 3	Interface 4
ESC:Exit-Text-Mode		Return to Page 1	

**Figure B-8. The Completed Page**

### Drawing a Box

For the first step, you'll draw one of the Interface boxes; the one on the far left. After completing this step, the application will look like Figure B-9.



**Figure B-9. Page 2 After the First Step**

When you draw this box, don't worry about being too exact. Keep in mind the general proportions: it should be large enough to enclose the text, and small enough to be duplicated three more times. Follow these steps from Page 2 of the application:

1. Select Backdrop from the screen legend.
2. Select Box-Mode.
3. Click on the position that will be the top left corner. A corner marker appears.
4. Click on the position that will be the bottom right corner. A second marker appears.
5. Select 1-Line-Box from the legend. The box is drawn.

### **Duplicating the Box**

The next is to duplicate this box and copy it three more times:

1. Click on the top left corner of the box you just drew. A marker appears on that corner of the box.
2. Click on the bottom right corner of the box. A second marker appears on that corner of the box.
3. Click Snip on the screen legend. You will see a screen message: Text Saved in Paste Buffer.
4. Click on the spot where you want the top left corner of the new box to appear. It should be a space or two to the right of the existing box.
5. Select Paste from the screen legend. The second box is drawn.

**Note:** The box remains in the memory buffer.

6. Paste the last two boxes in their positions.
7. Finish up by creating a large box around the four small boxes. After you define the corners, click on 2-Line-Box to create the double-line box.
8. Press [ESC] to exit Box-Mode.

### Drawing Lines

In this step, you will draw the lines across the top of the four small boxes:

1. Select Line-Mode from the screen legend.
2. Click on the left vertical line of the first box where you want the horizontal line to begin.
3. Press **f**. This creates the border/line character. To see a menu of all the available line characters and the keys to access them, select Keymap from the screen legend. These characters are not case sensitive. You will see the screen in Figure B-10.

Line Drawing Set											
Q	W	E	R	T	Y	U	I	O	-	=	[ ]
┌	┐	┑	┒	┓	└	┘	┙	┚	-	=	
A	S	D	F	G	H	J	K	L	1	2	3 4
┌	┐	┑	┒	┓	└	┘	┙	┚	▒	▓	▔ ▕
Z	X	C	U	B	N	M	.	;	5	6	7 8
┌	┐	┑	┒	┓	└	┘	┙	┚	■	▩	▪ ▫

**Figure B-10. Line Drawing Set**

4. Press “-” (hyphen character) repeatedly until you reach the right border.
5. Press **h** to draw the right-border character.
6. Repeat this for the other three boxes.
7. Press [ESC] to exit Line-Mode.

## Where to Go From Here

You've now used all of the basic procedures of the Custom Application tool. You're welcome to continue adding to or altering this sample application. The example suggests that you might build application menus specific to the interface cards, or create an application page for each interface with the appropriate jumps. Either way, you should have the basic skill set to create your own SNMP applications.

# Appendix C

## EAN 4000/SR 4200 Support

---

### Introduction

The EAN 4000 and SR 4200 support is used in conjunction with the EAN/Manager software installed on the CMS 400 network management system. EAN 4000 and SR 4200 support enables you to install, configure, monitor, and manage the EAN 4000 and SR 4200 units.

---

**Note:** No new option modules will be created to support the EAN 4000 and SR 4200 units. The EAN 4000 and SR 4200 units are included in the SNMP option module. The SNMP option key (LIM module) must be present to enable support for the EAN 4000 and SR 4200 units (SNMP\*.OPT).

---

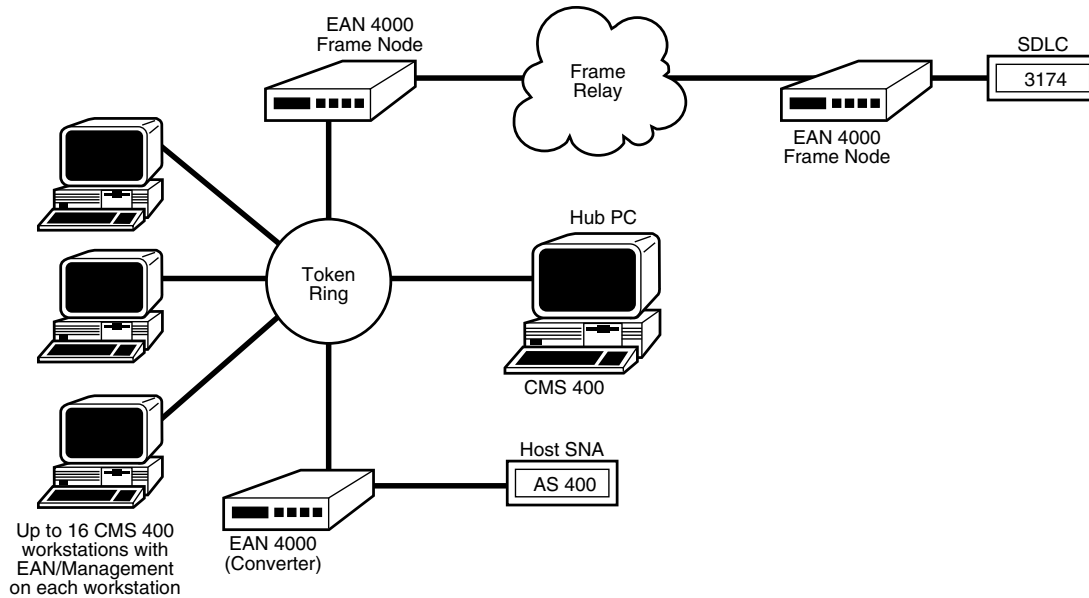
The EAN/Manager application (see Figure C-1) provides configuration management and monitoring of the EAN 4000 and SR 4200. This software runs on the CMS 400 PC (collapsed hub or workstation). If EAN/Manager software is not running, clicking on the icon automatically starts it. For specific information on your EAN/Manager application, refer to your *Sync/Manager™ 4.0 User's Guide* from Sync Research™. Figure C-1 shows an application of the EAN 4000 and SR 4200 using the CMS 400 network management system.

### About The EAN 4000 and SR 4200 Devices

The EAN 4200 is used when only a single protocol support is required. (No LAN support is available.) It also provides frame relay connectivity for up to 16 IBM SDLC or BSC controllers on one DTE serial port.

The EAN 4400 provides frame relay connectivity for up to 60 IBM SDLC and/or BSC controllers. The unit is available with one or three DTE serial ports. Additionally, an optional LAN port is available for SNA devices on a Token Ring or Ethernet LAN.

The SR 4200 is a rack mountable and software configurable device. The SR 4200 provides frame relay connectivity for up to 60 IBM SDLC and/or BSC controllers. The unit is available with up to seven DTE serial ports. Additionally, an optional LAN port is available for SNA devices on a Token Ring or Ethernet LAN.



**Figure C-1. EAN/Manager Application**

## Diagnostic Connectivity

The EAN 4000 and SR 4200 units are managed by using SNMP and Telnet protocols transported over TCP/IP on a LAN. The CMS 400 hub must have FTP's PC/TCP protocol stack installed. Each EAN 4000 and SR 4200 unit has its own connection to the LAN and a unique IP address on the network.

When running the CMS 400 as an expanded system (multiple workstations connected to a hub), traps are received by both the CMS 400 and the EAN/Manager. The EAN 4000 and SR 4200 units must be configured to send traps to both the CMS 400 hub IP address and the IP addresses of all of the workstations where the EAN/Manager application will run.

## About Traps

EAN 4000 and SR 4200 traps are recognized, parsed, and mapped to CMS 400 alarm types. The variables contained in an EAN 4000 and SR 4200 trap are mapped to text strings providing detailed information for the trap. The alarms appear in the alarm queue and can be viewed from the Alarms application.

The following table lists the EAN 4000 and SR 4200 traps from the MIB that CMS 400 will recognize.

---

**Note:** Trap numbers 808 through 816 are obsolete and are not supported.

---

Table C-1. EAN 4000 and SR 4200 Trap Types

Trap Number	Alarm Code	Additional Description in Alarm Parameters Field	Bindings In Alarm Parameters Field
6.800	<b>CNF</b> (Reconfiguration)	The configuration has changed.	Configuration ID
6.801	<b>ILC</b> (Illegal Configuration)	The configuration loaded is not valid.	Alarm Code <b>Note:</b> Refer to “Configuration Alarms” in Appendix A of your <i>FrameNode NMS Command Reference Guide</i> and <i>ConversionNode® User’s Guide</i> .
6.802	<b>INT</b> (Internal Event)	A memory core dump exists.	File Name
6.803	<b>INT</b> (Internal Event)	A memory dump has been retrieved.	None
6.804	<b>LDU</b> (Line Down/Up)	The line status has changed.	Port, Status, Alarm Code, and Cable Type
6.805	<b>LDU</b> (Line Down/Up)	The LAN status has changed.	Status, Alarm Code, and Cause Code
6.806	<b>SQL</b> (Signal Quality Level)	The line quality has changed.	Port, Frame Count, CRC Errors, and Aborts
6.807	<b>LDU</b> (Line Down/Up)	The PU status has changed.	Port, Status, PU Address, and Alarm Code
6.817	<b>ALT</b> (Alternate Line)	The session has switched to a primary DLCI.	Port, PU Address, and DLCI Number
6.818	<b>ALT</b> (Alternate Line)	The session has switched to a parallel DLCI.	Port, PU Address, and DLCI Number
6.819	<b>LKU</b> (Link Up)	The PU session on a primary DLCI is up.	Port, PU Address, DLCI Number, and MAC Address
6.820	<b>LKU</b> (Link Up)	The PU session on a parallel DLCI is up.	Port, PU Address, DLCI Number, and MAC Address
6.821	<b>LKU</b> (Link Up)	The PU session on an alternate DLCI is up.	Port, PU Address, DLCI Number, and MAC Address
6.822	<b>LKU</b> (Link Up)	The PU session on a primary MAC is up.	Port, PU Address, DLCI Number, and MAC Address

**Table C-1. EAN 4000 and SR 4200 Trap Types (Continued)**

<b>Trap Number</b>	<b>Alarm Code</b>	<b>Additional Description in Alarm Parameters Field</b>	<b>Bindings In Alarm Parameters Field</b>
6.823	<b>LKU</b> (Link Up)	The PU session on an alternate MAC is up.	Port, PU Address, DLCI Number, and MAC Address
6.824	<b>LKD</b> (Link Down)	The PU session on a primary MAC is down.	Port, PU Address, DLCI Number, MAC Address, and Diagnostic Code
6.825	<b>LKD</b> (Link Down)	The PU session on an alternate MAC is down	Port, PU Address, DLCI Number, MAC Address, and Diagnostic Code
6.826	<b>LCR</b> (Lost Communication with Remote)	The UNI connectivity is lost.	Port
6.827	<b>RCR</b> (Regained Communication with Remote)	The UNI connectivity is restored	Port
6.828	<b>ALT</b> (Alternate Line)	The system has switched the device to a switched backup connection on an alternate line.	Port
6.829	<b>LKU</b> (Link Up)	The system has switched the device to a dedicated line connection.	Port

## Diagnostic Code

Values that appear in the Diagnostic Code field are Call Clearing Codes. Descriptions of Call Clearing Codes are located in Appendix A of your *FrameNode NMS Command Reference Guide* (document number 878DFRMR4-10).

The Call Clearing Codes descriptions are also located in Appendix A of your *ConversionNode User's Guide* (document number 878DCONVR4-7).

## Cause Code

Values that appear in the Cause Code field are Token Ring LAN Failure Codes. Descriptions of Token Ring LAN Failure Codes are located in Appendix A of your *FrameNode NMS Command Reference Guide* (document number 878DFRMR4-10).

---

**Note:** Token Ring LAN Failure Codes are only applicable for trap 6.805.

---

Token Ring LAN Failure Codes descriptions are also located in Appendix A of your *ConversionNode User's Guide* (document number 878DCONVR4-7).

## Alarm Code

Values that appear in the Alarm Code field are listed under several sections in your *FrameNode NMS Command Reference Guide* and *ConversionNode User's Guide*. Trap 805 information is in the "Token Ring LAN Failure Codes" section (in the Phase/Error Code Combinations table). Trap 801 information is in the "Configuration Alarms" section. Trap 804 and 807 information is in the "SDLC Line / PU Failure Codes" section. For Trap 6.805, the alarm code is listed in the "Token Ring LAN Failure Code" section.

---

**Note:** SDLC Line / PU Failure Codes are only applicable for traps 6.801, 6,804, and 6.807.

---



# Index

---

<b>A</b>		
Alarms		
displaying for SNMP devices.....	4-3	
INX5000 device .....	4-4	
<b>B</b>		
Bridge parameters .....	3-16	
<b>C</b>		
Communities		
description .....	1-9	
Compile		
description .....	2-5	
Configure SNMP custom application .....	2-16	
Control		
operations .....	5-1	
Customization		
parameters .....	3-21	
<b>D</b>		
Database		
adding INX5000 units .....	3-3	
deleting INX5000 units .....	3-4	
modifying INX5000 units .....	3-3	
Directing MIB variables		
INX5000.....	5-1	
<b>E</b>		
Ethernet buses		
INX5000 chassis .....	4-4	
moving in INX5000 .....	3-4	
statistics .....	4-4	
<b>G</b>		
GET/SET		
directing.....	5-5	
<b>H</b>		
Handler definition		
description .....	3-22	
Health table		
adding .....	2-7	
creating .....	2-5	
deleting .....	2-8	
modifying .....	2-8	
<b>I</b>		
Inserting		
new unit .....	1-11	
INX 10 Base T		
filter .....	3-5	
statistics .....	4-6	
INX 10 Base T repeater		
thresholds .....	3-6	
INX Managed 10 Base T Repeater		
changing name.....	3-6	
INX T-Ring CAU		
configure port .....	3-12	
display unit .....	4-6	
examining .....	4-16	
name change .....	3-13	
thresholds .....	3-13	
INX4000		
name change .....	3-14	
parameters .....	3-16	
port change .....	3-15	
thresholds .....	3-18	
INX5000		
adding units .....	3-3	
alarms .....	4-4	
closing .....	5-2	
deleting units .....	3-4	
directing MIB variables.....	5-1	
display device .....	3-2	
displaying device.....	4-3	
Ethernet buses .....	4-4	
examining .....	4-14	
MIB configuration.....	3-2	
modifying units .....	3-3	
monitor devices .....	4-10	
move Ethernet buses.....	3-4	
move internal buses .....	3-4	
opening .....	5-2	
rebooting.....	5-3	

- reinitialize.....5-3
- rotating .....5-2
- INX-FOIRL
  - statistics .....4-6
- INX-MGR
  - statistics .....4-6
- INX-NTS
  - configure port .....3-8
  - display parameters .....3-7
  - modify parameters .....3-7
  - name change .....3-11
  - port configuration .....3-8
  - thresholds .....3-11
- IP addresses
  - alternate .....2-11
  - discovering .....1-7
  - Scan Range window .....1-7
- M**
- Masking traps .....2-10
- MIB
  - displaying objects .....5-5
  - Top-16 monitor .....4-9
  - Viewing object values .....4-2
- N**
- Naming
  - INX T-Ring CAU .....3-13
- Network Interface Card .....1-4
- Network Map
  - adding units .....1-11
- O**
- Options
  - report .....4-12, 4-16
- P**
- Pinging an SNMP device .....5-3
- Port
  - INX T-Ring CAU configure .....3-12
  - INX-NTS configure .....3-8
- Ports on an SNMP Device
  - enabling/disabling .....5-3
- Proxy Agents
  - setting parameters .....1-10

- R**
- Reboot an SNMP device .....5-4
- Rebooting INX5000 module .....5-3
- Reinitializing an INX5000 .....5-3
- Rename SNMP application .....2-15
- Repeater
  - changing name of INX 10 Base T .....3-6
- Reporting
  - options .....4-12
- Reporting options .....4-16
- Requirements
  - hardware .....1-2
  - software .....1-2
- RFCs
  - FTP site .....2-2
- RNX6300
  - configure console .....3-20
  - console .....5-5
- RNX6x00
  - panel .....5-4
- RNX6x00/6150
  - configuration .....3-19
  - maintenance statistics .....4-20
  - monitor .....4-16
  - traffic statistics .....4-19
- Router
  - monitor RNX6x00/6150 .....4-16
- S**
- SNMP
  - add application .....2-12
  - communities .....1-8
  - configure application .....2-16
  - delete application .....2-15
  - displaying a device .....4-2
  - general setup .....1-9
  - getting more information .....2-1
  - groups .....1-9
  - health table .....2-5
  - modify application .....2-15
  - rename application .....2-15
  - sites .....1-9
  - top-16 monitor .....4-9
  - traps .....2-8
  - user-defined applications .....2-12
- Statistics
  - displaying for SNMP devices .....4-3
- System

---

parameters .....	3-21
<b>T</b>	
TCP/IP	
installation .....	1-5
Telnet	
accessing .....	5-6
from T-Ring CAU .....	5-4
Thresholds	
INX 10 Base T repeater .....	3-6
INX T-Ring CAU .....	3-13
INX4000 bridge .....	3-18
INX-NTS .....	3-11
Top-16 Monitor .....	4-9
setting up .....	4-9
Traffic statistics	
RNX6x00/6150 .....	4-19
Trap	
deleting .....	2-11
masking .....	2-10
T-Ring CAU Telnet	
accessing .....	5-4



**We want your feedback.**

To better serve our customers, Milgo Solutions welcomes your comments concerning this manual. Please take the time to fill out the following questionnaire, remove it from your manual, and drop it in the mail or FAX it to us at (954) 846-3244. We also welcome your comments via e-mail at address *techdoc@milgo.com*.

Name of Manual/Document No./Date:

CMS 400 LAN Internetworking Manager User's Guide, 13D36A-7/D, 11/96

Was the information in this manual presented in a logical order?

\_\_\_\_\_ Excellent      \_\_\_\_\_ Good      \_\_\_\_\_ Fair      \_\_\_\_\_ Poor

How easy was it to locate specific information?

\_\_\_\_\_ Very easy      \_\_\_\_\_ Moderately easy      \_\_\_\_\_ Difficult

Rate the technical level of information presented in this manual:

\_\_\_\_\_ Too technical      \_\_\_\_\_ Suitable technical level      \_\_\_\_\_ Not technical enough

Are technical terms clearly defined?

\_\_\_\_\_ Excellent      \_\_\_\_\_ Good      \_\_\_\_\_ Fair      \_\_\_\_\_ Poor

Rate the quality of the illustrations:

\_\_\_\_\_ Excellent      \_\_\_\_\_ Good      \_\_\_\_\_ Fair      \_\_\_\_\_ Poor

Are the manual's instructions clearly written?

\_\_\_\_\_ Excellent      \_\_\_\_\_ Good      \_\_\_\_\_ Fair      \_\_\_\_\_ Poor

Rate the quantity of the illustrations in this manual:

\_\_\_\_\_ Too many      \_\_\_\_\_ Suitable amount      \_\_\_\_\_ Not enough

Does this manual contain all the information you require? (Y/N)

If not, what would you suggest we add to make the manual more useful?

---

---

---

Did you find any errors in this manual? (Y/N)

If yes, please note the error and page number in the space provided below:

---

---

---

NAME \_\_\_\_\_ TITLE \_\_\_\_\_

COMPANY \_\_\_\_\_

ADDRESS \_\_\_\_\_

CITY \_\_\_\_\_ STATE \_\_\_\_\_ ZIP \_\_\_\_\_

TELEPHONE NO. (    ) \_\_\_\_\_

Tape Here

- FOLD



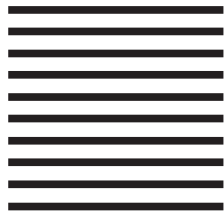
No  
Postage Stamp  
Necessary  
If Mailed In The  
United States

**BUSINESS REPLY MAIL**  
FIRST CLASS MAIL PERMIT NO. 8699, FT. LAUDERDALE, FLORIDA

Postage Will Be Paid By Addressee

**MILGO Solutions, Inc.**

Attn: Technical Writing, MS-D108  
Post Office Box 407044  
Fort Lauderdale, FL 33340-7044



-