7123 SNMP DSU/CSU

User's Guide

Document No. 7123-A2-GB20-00

September 2001

PARADYNE®

Copyright © 2001 Paradyne Corporation
All rights reserved.
Printed in U.S.A.

Notice

This publication is protected by federal copyright law. No part of this publication may be copied or distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language in any form or by any means, electronic, mechanical, magnetic, manual or otherwise, or disclosed to third parties without the express written permission of Paradyne Corporation, 8545 126th Ave. N., Largo, FL 33773.

Paradyne Corporation makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Further, Paradyne Corporation reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation of Paradyne Corporation to notify any person of such revision or changes.

Changes and enhancements to the product and to the information herein will be documented and issued as a new release to this manual.

Warranty, Sales, Service, and Training Information

Contact your local sales representative, service representative, or distributor directly for any help needed. For additional information concerning warranty, sales, service, repair, installation, documentation, training, distributor locations, or Paradyne worldwide office locations, use one of the following methods:

- **Internet:** Visit the Paradyne World Wide Web site at **www.paradyne.com**. (Be sure to register your warranty at **www.paradyne.com/warranty**.)
- **Telephone:** Call our automated system to receive current information by fax or to speak with a company representative.
  - — Within the U.S.A., call 1-800-870-2221
  - — Outside the U.S.A., call 1-727-530-2340

Document Feedback

We welcome your comments and suggestions about this document. Please mail them to Technical Publications, Paradyne Corporation, 8545 126th Ave. N., Largo, FL 33773, or send e-mail to **userdoc@paradyne.com**. Include the number and title of this document in your correspondence. Please include your name and phone number if you are willing to provide additional clarification.

Trademarks

ACCULINK, COMSPHERE, FrameSaver, Hotwire, MVL, NextEDGE, OpenLane, and Performance Wizard are registered trademarks of Paradyne Corporation. ReachDSL and TruePut are trademarks of Paradyne Corporation. All other products and services mentioned herein are the trademarks, service marks, registered trademarks, or registered service marks of their respective owners.

Contents

About This Guide

- Purpose and Intended Audience v
- Document Organization v
- Product-Related Documents vi
- Conventions Used vii

1 About the 7123 SNMP DSU/CSU

- System Overview 1-1
- Differences Between 7112 and 7123 DSU/CSUs 1-2

2 User Interface and Basic Operation

- Logging On. 2-2
- Main Menu 2-4
- Screen Work Areas 2-5
- Navigating the Screens 2-6
  - Keyboard Keys 2-6
  - Function Keys 2-7
  - Selecting from a Menu. 2-8
  - Switching Between Screen Areas 2-8
  - Selecting a Field 2-9
  - Entering Information 2-9

3 Configuration

- Basic Configuration 3-2
  - Configuration Option Areas 3-3
  - Accessing and Displaying Configuration Options 3-4
  - Changing Configuration Options 3-5
  - Saving Configuration Options 3-6
- Entering System Information and Setting the System Clock 3-7
- Configuration Option Tables 3-8
- Configuring the Overall System 3-9
  - Configuring General System Options 3-9

- Configuring the Physical Interfaces 3-10
  - Configuring the Network Interface 3-10
  - Configuring the User Data Port 3-13
- Assigning Time Slots/Cross Connections 3-16
  - Assigning the Synchronous Data Port to Network Time Slots 3-17
  - Clearing Assignments 3-18
- Setting Up Management and Communication Options 3-19
  - Configuring Node IP Information 3-19
  - Configuring General SNMP Management 3-21
  - Configuring Telnet and/or FTP Session Support 3-22
  - Configuring SNMP NMS Security 3-25
  - Configuring SNMP Traps 3-27
  - Configuring the Ethernet Port 3-30
  - Configuring the Communication Port 3-32
  - Configuring the COM Port to Support an External Modem 3-36

4 Security and Logins

- Limiting Access 4-2
- Controlling Asynchronous Terminal Access 4-2
- Controlling External COM Port Device Access 4-4
- Controlling Telnet or FTP Access 4-4
  - Limiting Telnet Access 4-5
  - Limiting FTP Access 4-6
- Controlling SNMP Access 4-7
  - Disabling SNMP Access 4-7
  - Assigning SNMP Community Names and Access Levels 4-8
  - Limiting SNMP Access through IP Addresses 4-9
- Creating a Login 4-10
- Modifying a Login 4-11
- Deleting a Login 4-11

5 Operation and Maintenance

- Displaying System Information 5-2
- Viewing LEDs and Control Leads 5-3
  - LED Descriptions 5-4
- Device Messages 5-6
- Status Information 5-10
  - System and Test Status Messages 5-11
  - Time Slot Assignment Status 5-14

- IP Routing Table 5-15
- Performance Statistics 5-17
  - Clearing Performance Statistics 5-18
  - ESF Line Performance Statistics 5-19
  - Ethernet Performance Statistics 5-22
- FTP File Transfers 5-23
  - Upgrading System Software 5-25
  - Determining Whether a Download Is Complete. 5-26
  - Changing Software 5-26

6 Troubleshooting

- Problem Indicators 6-2
- Resetting the Unit and Restoring Communication 6-3
  - Resetting the Unit from the Control Menu 6-3
  - Resetting the Unit By Cycling the Power 6-3
  - Restoring Communication with an Improperly Configured Unit . . . 6-4
- Alarms 6-5
- Troubleshooting Device Problems 6-8
- Tests Available 6-9
  - Test Timeout Feature 6-10
- Starting and Stopping a Test 6-10
  - Aborting All Tests. 6-11
- Physical Tests 6-12
  - Line Loopback 6-13
  - Payload Loopback 6-14
  - Send Line Loopback 6-15
  - Send and Monitor Pattern Tests 6-16
  - DTE Loopback 6-17
- IP Ping Test 6-18
- Lamp Test 6-19

A Menu Hierarchy

- Menus A-1

B SNMP MIBs and Traps

- MIB Support B-2
- Downloading MIBs and SNMP Traps. B-2
- System Group (mib-2) B-3
  - DSU/CSU's sysDescr (system 1) B-3
  - DSU/CSU's sysObjectID (system 2) B-3
- Interfaces Group (mib-2) B-4
  - Paradyne Indexes to the Interface Table (ifTable). B-4
- Standards Compliance for SNMP Traps B-4
  - Trap: warmStart B-5
  - Trap: authenticationFailure B-5
  - Traps: linkUp and linkDown B-6
  - Traps: enterprise-Specific B-9
  - Physical Interface Alarm Defaults B-10

C Connectors, Cables, and Pin Assignments

- Front Panel. C-1
- Rear Panel C-1
- T1 Network Interface C-2
  - T1 Network Cable (Feature No. 3100-F1-500) C-2
  - Canadian T1 Line Interface Cable (Feature No. 3100-F1-510) . . . C-2
- COM Port Connector C-3
  - Standard EIA-232-D Crossover Cable. C-4
  - Configuring an External Modem C-5
- Data Port Connector C-6
  - Standard V.35 Straight-through Cable. C-6
- Ethernet Port Connector C-7

D Technical Specifications

E Equipment List

- Equipment E-1
- Cables E-2

Index

About This Guide

Purpose and Intended Audience

This document contains information that applies to the 7123 SNMP DSU/CSU unit. It is intended for system designers, engineers, administrators, and operators.

The reader should be familiar with the functional operation of digital data communications equipment.

Document Organization

Section	Description
Chapter 1, *About the 7123 SNMP DSU/CSU*	Describes some of the features of the 7123 DSU/CSU, including differences between it and the 7112 DSU/CSU.
Chapter 2, *User Interface and Basic Operation*	Shows how to navigate the menu-driven user interface.
Chapter 3, *Configuration*	Provides configuration information for the DSU/CSU.
Chapter 4, *Security and Logins*	Provides procedures for controlling access to the DSU/CSU and setting up logins.
Chapter 5, *Operation and Maintenance*	Provides procedures to display unit identification information and perform file transfers, as well as how to display and interpret status and statistical information.
Chapter 6, *Troubleshooting*	Provides device problem resolution, alarm, and other information, as well as troubleshooting and test procedures.
Appendix A, *Menu Hierarchy*	Contains a graphical representation of how the user interface screens are organized.
Appendix B, *SNMP MIBs and Traps*	Identifies the MIBs supported and how they can be downloaded, describes the unit's compliance with SNMP format standards and with its special operational trap features, and describes the alarm and event defaults.

Section	Description
Appendix C, *Connectors, Cables, and Pin Assignments*	Shows the rear panel, tells what cables are needed, and provides pin assignments for interfaces and cables.
Appendix D, *Technical Specifications*	Technical Specifications.
Appendix E, *Equipment List*	Equipment List.
Index	Lists key terms, acronyms, concepts, and sections.

A master glossary of terms and acronyms used in Paradyne documents is available on the World Wide Web at **www.paradyne.com**. Select *Library* → *Technical Manuals* → *Technical Glossary.*

Product-Related Documents

Document Number	Document Title
7123-A2-GN10	*7123 SNMP DSU/CSU Installation Instructions*

Paradyne OpenLane SLM NMS Documentation:

7800-A2-GB30	*OpenLane SLM Reports Reference Guide*
7800-A2-GB31	*OpenLane SLM Administrator's Guide*

Complete Paradyne documentation for this product is available at **www.paradyne.com**. Select *Library* → *Technical Manuals.*

To order a paper copy of this manual:

- Within the U.S.A., call 1-800-PARADYNE (1-800-727-2396)
- Outside the U.S.A., call 1-727-530-8623

Conventions Used

Convention	Used to . . .
Italic	Indicate variable information (for example, N*tt*).
Menu selection sequence	Provide an abbreviated method for indicating the selections to be made from a menu or selections from within a menu before performing a procedural step. For example, *Main Menu* → *Status* → *System and Test Status* indicates that you should select Status from the Main Menu, then select System and Test Status from the Status menu.
(Path:)	Provide a check point that coincides with the menu path shown at the top of the screen. Always shown within parentheses so you can verify that you are referencing the correct table (for example, Path: main/config/alarm).
Brackets [ ]	Indicate multiple selection choices when multiple options can be displayed (for example, Clear [*Network/Port-1*] Statistics).
Text highlighted in blue	Indicate a hyperlink to additional information when viewing this manual online. Click on the highlighted text.

About the 7123 SNMP DSU/CSU

1

System Overview

The 7123 SNMP DSU/CSU provides an interface between the T1 digital network and the customer premises equipment, converting signals received from the DTE (Data Terminal Equipment) to bipolar signals that can be transmitted over T1 lines.

The 7123 SNMP DSU/CSU offers these features:

- **Auto-Sensing 10/100BaseT Port.** Allows the DSU/CSU to connect directly to an Ethernet LAN.
- **SNMP (Simple Network Management Protocol) Management.** Provides network management via an industry-standard SNMP management system.
- **ASCII Terminal Interface.** Provides a menu-driven VT100-compatible interface for configuring and managing the DSU/CSU locally or remotely by Telnet session or External Modem.
- **Two Customer-Specified Configuration Storage Areas.** Allows quick access to alternate sets of configuration options.
- **Dual Flash Memory.** Allows software upgrades while the unit is up and running. Two software loads can be stored and implemented at the user's discretion.
- **Testing Capability.** Provides a variety of tests to identify and diagnose device and network problems. Tests can be commanded from the unit's menu-driven user interface or the OpenLane SLM system.
- **IP Routing Table.** Shows the IP routing table for the DSU/CSU, with network as well as host routes, the number of hops to the destination, the method by which the route was added to the table, the interface used to get to the destination, and how long the route has been in existence.

Differences Between 7112 and 7123 DSU/CSUs

If you have both models in your network, you should be aware that the 7112 DSU/CSU and 7123 DSU/CSU provide the same basic functions, but are based on different hardware platforms. The following table shows the major differences.

Feature	**7112**	**7123**
COM Port Default Data Rate	9.6 Kbps	19.2 Kbps
Data Port LEDs	TXT, RXD, RTS, CTS, DTR	TXT, RXD, RTS, DTR
Data Port Tests	Data Terminal (DTE) Loopback and Data Channel Loopback, Send V.54 and Send FT1 Loopbacks, Pattern Tests	DTE Loopback
DS0 Assignment by Block or ACAMI	Yes	No
FDL (Facility Data Link) for Remote Management	Yes	No
Front Panel Monitor Jacks	Yes	No
FTP Software and Configuration File Transfer	No	Yes
IP Ping	No	Yes
IP Routing Table Display	No	Yes
Management Protocol Statistics	Yes	No
Repeater Loopback Network Test	Yes	No
Software Upgrades	No	Two software versions can be stored and activated

User Interface and Basic Operation

2

This chapter tells you how to access, use, and navigate the menu-driven user interface. It includes the following:

- *Logging On* on page 2-2
- *Main Menu* on page 2-4
- *Screen Work Areas* on page 2-5
- *Navigating the Screens* on page 2-6
  - *Keyboard Keys*
  - *Function Keys*
  - *Selecting from a Menu*
  - *Switching Between Screen Areas*
  - *Selecting a Field*
  - *Entering Information*

What appears on the screens depends on:

- **Current configuration** – How your network is currently configured.
- **Security access level** – The security level set by the system administrator for each user.
- **Data selection criteria** – What you entered in previous screens.

Logging On

Start a session using one of the following methods:

- Telnet session via the Ethernet port.
- Dial-in connection using an external modem.
- Direct terminal connection over the COM port.

When logging on, the User Interface Idle screen appears.

- If no security was set up or security was disabled, the Main Menu screen appears (see *Main Menu* on page 2-4). You can begin your session.
- If security was set up and is enabled, you are prompted for a login. Enter your login ID and password.

When the user interface has been idle, a session is automatically ended and the screen goes blank when the unit times out. Press Enter to reactivate the interface.

▶ Procedure

To log in when security is being enforced:

1. Type your assigned Login ID and press Enter.
2. Type your Password and press Enter.

   — Valid characters – All printable ASCII characters

   — Number of characters – Up to 10 characters can be entered in the Login ID and Password fields

   — Case-sensitive – Yes

   An asterisk (*) appears in the password field for each character entered.

If your login was . . .	Then the . . .
Valid	*Main Menu* appears. Begin your session. **NOTE:** If your login is valid, but access is denied, there are two currently active sessions.
Invalid	Message, **`Invalid Password`**, appears on line 24, and the Login screen is redisplayed. After three unsuccessful attempts: ■ A Telnet session is closed. ■ The User Interface Idle screen appears for a directly connected terminal or modem. ■ An SNMP trap is generated. Access is denied. See your system administrator to verify your login (Login ID/Password combination).

The 7123 DSU/CSU supports two simultaneous sessions. If two sessions are currently active, wait and try again.

- If two sessions are currently active and you are attempting to access the unit through Telnet, the local Telnet client process returns a **`Connection refused:`** message at the bottom of the screen.
- If two sessions are currently active and you are attempting to access the unit over the COM port (using a terminal or external modem, not via Telnet), the User Interface Already In Use screen is redisplayed. In addition, the type of connection (Telnet Connection or Direct COM Port Connection) for each current user is identified, along with the user's login ID.

▶ Procedure

To end the session:

1. Press Ctrl-a to switch to the function keys area of the screen.
2. Type **e** (Exit) and press Enter.
   - — For a terminal-connected to the COM port, the session is ended.
   - — For a modem connected to the COM port, the session is ended and the modem is disconnected.
   - — For a Telnet connection, the session is closed and, if no other Telnet or FTP session is occurring over the connection, the modem is disconnected.

If ending a session from the Configuration branch, see *Saving Configuration Options* in Chapter 3, *Configuration*.

Main Menu

Entry to all of the DSU/CSU's tasks begins at the Main Menu, which has several menus or branches.

Access Level appears at the top of the screen if security has been set up.

```
main                              Access Level: 1                          7123
Device Name: Node A                                                09/09/2001 02:01

                                   MAIN MENU

                                  Status
                                  Test
                                  Configuration
                                  Control

--------------------------------------------------------------------------------
Ctrl-a to access these functions                                          Exit
```

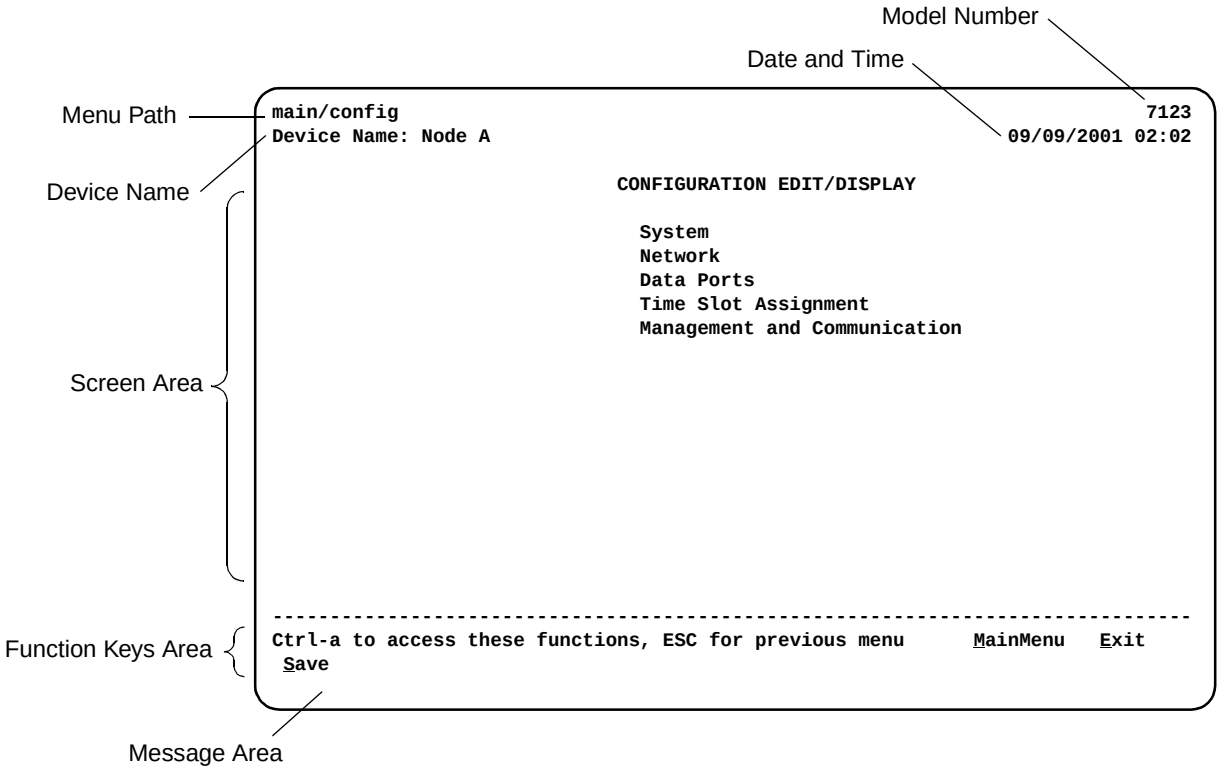
Select . . .	To . . .
Status	View diagnostic tests, interfaces, and statistics. You can also display LEDs and DSU/CSU identity information.
Test	Select and cancel tests for the DSU/CSU's interfaces.
Configuration	Display and edit the configuration options.
Control	Control the menu-driven user interface, device naming, login administration, and selecting software releases. You can also initiate a power-on reset of the DSU/CSU.

See Appendix A, *Menu Hierarchy*, for a pictorial view of the menu hierarchy, which represents the organization of the DSU/CSU's menus and screens.

Screen Work Areas

There are two user work areas:

- **Screen area** – Where you input information into fields.
- **Function keys area** – Where you perform specific screen functions.



Screen Format	Description
Menu Path	Menu selections made to reach the current screen.
Device Name	Customer-assigned identification of the DSU/CSU.
7123	The DSU/CSU's model number.
Screen Area	Selection, display, and input fields for monitoring and maintaining the DSU/CSU.
Function Keys Area	Specific functions that can be performed by pressing a specified key, then pressing Enter.
Message Area	System-related information and valid settings for input fields in the lower left corner. System and Test Status messages in the lower right corner.

Navigating the Screens

You can navigate the screens by:

- Using keyboard keys.
- Switching between the two screen work areas using function keys.

Keyboard Keys

Use the following keyboard keys to navigate within the screen area:

Press . . .	**To . . .**
Ctrl-a	Move cursor between the screen area and the screen function keys area.
Esc	Return to the previous screen.
Right Arrow (on same screen row), or Tab (on any screen row)	Move cursor to the next field.
Left Arrow (on same screen row), or Ctrl-k	Move cursor to the previous field.
Backspace	Move cursor one position to the left or to the last character of the previous field.
Spacebar	Select the next valid value for the field.
Delete (Del)	Delete character that the cursor is on.
Up Arrow or Ctrl-u	Move cursor up one field within a column on the same screen.
Down Arrow or Ctrl-d	Move cursor down one field within a column on the same screen.
Right Arrow or Ctrl-f	Move cursor one character to the right if in edit mode.
Left Arrow or Ctrl-b	Move cursor one character to the left if in edit mode.
Ctrl-l	Redraw the screen display, clearing information typed in but not yet entered.
Enter (Return)	Accept entry or, when pressed before entering data or after entering invalid data, display valid options on the last row of the screen.

Function Keys

All function keys (located in the lower part of the screen; see the example in *Screen Work Areas* on page 2-5) operate the same way throughout the screens. They are not case-sensitive, so upper- or lowercase letters can be used interchangeably.

These keys use the following conventions:

Select . . .	For the screen function . . .	And press Enter to . . .
M or m	MainMenu	Return to the Main Menu screen.
E or e	Exit	Terminate the menu-driven user interface session.
N or n	New	Enter new data.
O or o	Modify	Modify existing data.
L or l	DeIete	Delete data.
S or s	Save	Save information.
R or r	Refresh	Update screen with current information.
C or c	ClrStats	Clear network performance statistics and refresh the screen.
U or u	PgUp	Display the previous page.
D or d	PgDn	Display the next page.

Selecting from a Menu

▶ Procedure

To select from a menu:

1. Tab or press the down arrow key (↓) to position the cursor on a menu selection, or press the up arrow key (↑) to move the cursor to the bottom of the menu list.

   Each menu selection is highlighted as you press the key to move the cursor from position to position.

2. Press Enter. The selected menu or screen appears.

▶ Procedure

To return to a previous screen, press the Escape (Esc) key until you reach the desired screen.

Switching Between Screen Areas

Use Ctrl-a to switch between screen areas (see *Screen Work Areas* on page 2-5).

▶ Procedure

To switch to the function keys area:

1. Press Ctrl-a to switch from the screen area to the function keys area.
2. Select either the function's designated (underlined) character or Tab to the desired function key.
3. Press Enter. The function is performed.

To return to the screen area, press Ctrl-a again.

Selecting a Field

Once you reach the desired menu or screen, select a field to view or change, or issue a command.

Press the Tab or right arrow key to move the cursor from one field to another. The current setting or value appears to the right of the field.

Entering Information

You can enter information in one of three ways. Select the field, then:

- Manually type in (enter) the field value or command.

  Example:
  Entering **admin** as a user's Login ID on the Administer Logins screen (from the Control menu/branch).

- Type in (enter) the first letter(s) of a field value or command, using the unit's character-matching feature.

  Example:
  When configuring a port's physical characteristics with the Port (DTE) Initiated Loopbacks configuration option/field selected (possible settings include Disable, Local, DTPLB, DCLB, and Both), entering **d** or **D** displays the first value starting with d – Disable. In this example, entering **dt** or **DT** would display DTPLB as the selection.

- Switch to the function keys area and select or enter a designated function key.

  Example:
  To save a configuration option change, select Save. S or s is the designated function key.

If a field is blank and the Message area displays valid selections, press the spacebar; the first valid setting for the field appears. Continue pressing the spacebar to scroll through other possible settings.

Configuration

3

This chapter includes the following:

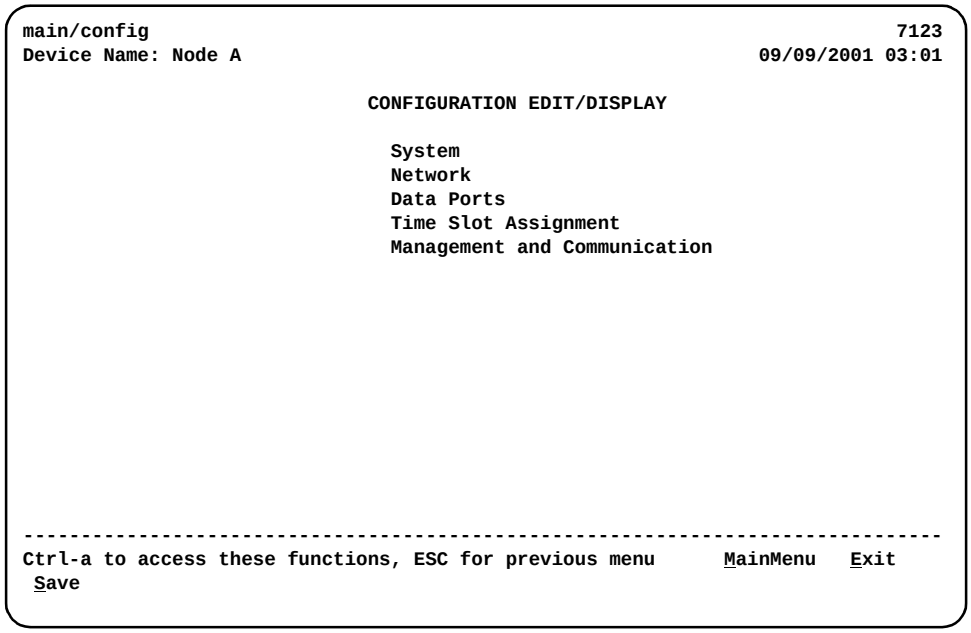
- *Basic Configuration* on page 3-2
  - *Configuration Option Areas*
  - *Accessing and Displaying Configuration Options*
  - *Changing Configuration Options*
  - *Saving Configuration Options*
- *Entering System Information and Setting the System Clock* on page 3-7
- *Entering System Information and Setting the System Clock* on page 3-7
- *Configuration Option Tables* on page 3-8
- *Configuring the Overall System* on page 3-9
- *Configuring the Physical Interfaces* on page 3-10
  - *Configuring the Network Interface*
  - *Configuring the User Data Port*
- *Assigning Time Slots/Cross Connections* on page 3-16
  - *Assigning the Synchronous Data Port to Network Time Slots*
  - *Clearing Assignments*
- *Setting Up Management and Communication Options* on page 3-19
  - *Configuring Node IP Information*
  - *Configuring General SNMP Management*
  - *Configuring Telnet and/or FTP Session Support*
  - *Configuring SNMP NMS Security*
  - *Configuring SNMP Traps*
  - *Configuring the Ethernet Port*
  - *Configuring the Communication Port*
  - *Configuring the COM Port to Support an External Modem*

Basic Configuration

Configuration option settings determine how the 7123 SNMP DSU/CSU operates. Use the DSU/CSU's Configuration Edit/Display menu to display or change configuration option settings.

The Configuration Edit/Display menu of the 7123 DSU/CSU is shown below.

Configuration Menu



Configuration Option Areas

The DSU/CSU arrives with configured factory default settings, which are located in the Factory Default Configuration option area. You can find the default settings for configuration options in the *Configuration Option Tables* on page 3-8.

If the factory default settings do not support your network's configuration, you can customize the configuration options to better suit your application.

Four configuration option storage areas are available:

Configuration Option Area	Description
Current Configuration	The currently active set of configuration options.
Customer Configuration 1	An alternate set of configuration options that the customer can set up and store for future use.
Customer Configuration 2	Another alternate set of configuration options that the customer can set up and store for future use.
Default Factory Configuration	A read-only configuration area containing the factory default set of configuration options. You can load and edit default factory configuration settings, but you can only save those changes to the Current, Customer 1, or Customer 2 configuration option areas. The Current, Customer 1, and Customer 2 configuration option areas are identical to the Default Factory Configuration until modified by the customer.

Accessing and Displaying Configuration Options

To access and display configuration options, load (copy) the applicable configuration option set into the edit area.

▶ Procedure

To load a set of configuration options for editing:

1. From the Main Menu, press the down arrow key (↓) so the cursor is on Configuration.
2. Press Enter to display the Configuration menu. The **Load Configuration From:** menu appears.
3. Select the configuration option area from which you want to load configuration options and press Enter (Current Configuration, Customer Configuration 1, Customer Configuration 2, or Default Factory Configuration).

   The selected set of configuration options is loaded into the configuration edit area and the **Configuration Edit/Display** menu appears.

This sequence of steps would be shown as the menu selection sequence:

Main Menu → Configuration

Changing Configuration Options

▶ Procedure

To change configuration option settings:

1. From the **Configuration Edit/Display** menu, select a set of configuration options and press Enter.

   For example:
   Configuration → Data Ports

2. Select the configuration options that are applicable to your network, and make appropriate changes to the setting(s). See Chapter 2, *User Interface and Basic Operation*, for additional information.

3. Repeat Steps 1 and 2 until all changes are complete.

NOTE:

— Only Security Access Level 1 users can change configuration options.

— Security Access Level 2 users can only view configuration options and run tests.

— Security Access Level 3 users can only view configuration options; they cannot change configuration options or run tests.

Saving Configuration Options

When changes to the configuration options are complete, use the Save function key to save your changes to either the Current, Customer 1, or Customer 2 configuration areas.

NOTE:

When changing settings, you must Save for changes to take effect.

▶ Procedure

To save the configuration option changes:

1. Press Ctrl-a to switch to the function key area at the bottom of the screen.
2. Type **s** or **S** to select the Save function and press Enter.

   The **Save Configuration To:** screen appears.

   NOTE:

   If you try to exit the Configuration menu without saving changes, a Save Configuration screen appears requiring a Yes or No response.

   — If you select No, the Main Menu screen reappears and the changes are not saved.

   — If you select Yes, the **Save Configuration To:** screen appears.
3. Select the configuration option area to which you want to save your changes (usually the Current Configuration) and press Enter.

   When Save is complete, **`Command Complete`** appears in the message area at the bottom of the screen.

   NOTE:

   There are other methods of changing configurations, like SNMP and Auto-Configuration. Since multiple sessions can be active at the same time, the last change made overwrites any previous or current changes being made. For instance:

   — Saving your configuration changes would cause configuration changes made via another method to be lost.

   — If you are making changes and someone else makes changes and saves them, your changes would be lost.

Entering System Information and Setting the System Clock

Select System Information to set up or display the general SNMP name for the unit, its location, and a contact for the unit, as well as to set the system clock.

Main Menu → Control → System Information

The following information is available for viewing. Save any entries or changes.

If the selection is . . .	Enter the . . .
Device Name	Unique name for device identification of up to 20 characters.
System Name	SNMP system name; can be up to 255 characters.
System Location	System's physical location; can be up to 255 characters.
System Contact	Name and how to contact the system person; can be up to 255 characters.
Date	Current date in the month/day/year format (mm/dd/yyyy).
Time	Current time in the hours:minutes format (hh:mm).

NOTE:

To clear existing information, place the cursor in the Clear field (Tab to the Clear field) and press Enter.

See Chapter 4, *Security and Logins,* to set up and administer logins.

Configuration Option Tables

Configuration option descriptions contained in this chapter are in menu order, even though this may not be the order in which you access each when configuring the unit.

The following configuration option tables are included:

- Table 3-1, General System Options
- Table 3-2, Network Physical Interface Options
- Table 3-3, Data Port Physical Interface Options
- Table 3-4, Node IP Options
- Table 3-5, General SNMP Management Options
- Table 3-6, Telnet and FTP Session Options
- Table 3-7, SNMP NMS Security Options
- Table 3-8, SNMP Traps Options
- Table 3-9, Ethernet Management Options
- Table 3-10, Communication Port Options
- Table 3-11, External Modem (COM Port) Options

Configuring the Overall System

The following section describes how to configure the System menu options:

- *Configuring General System Options*

Configuring General System Options

Select General from the System menu to configure the general system configuration options (see Table 3-1, General System Options).

Main Menu → *Configuration* → *System* → *General*

Table 3-1. General System Options

Test Timeout
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether or not loopback and pattern tests have a duration after which they are terminated automatically. This setting does not effect DTE-commanded tests or the LMI Packet Capture Utility feature. **Enable** – All Loopback and Pattern tests have a timeout. **Disable** – Loopback and pattern tests must be manually terminated.
Test Duration (min)
Possible Settings: **1 – 120** Default Setting: **10**
Specifies the maximum duration of user-initiated tests. *Display Conditions* – This option only appears when Test Timeout is set to Enable. **1 – 120** – Sets the Test Timeout period in minutes (inclusive).
Primary Clock Source
Possible Settings: **Net1, Internal** Default Setting: **Net1**
Allows you to select the primary clock source for the unit. The source selected provides all of the timing within the DSU/CSU and the clocks for all of the external interfaces. **Net1** – The primary clock is derived from the Network1 interface. **Internal** – The primary clock is the internal clock.

Configuring the Physical Interfaces

The following sections describe how to configure the characteristics for physical interfaces:

- *Configuring the Network Interface*
- *Configuring the User Data Port*

Configuring the Network Interface

When configuring the physical characteristics for the network interface, select Physical from the Network menu (see Table 3-2, Network Physical Interface Options).

Main Menu → *Configuration* → *Network* → *Physical*

Table 3-2. Network Physical Interface Options (1 of 3)

Line Framing Format
Possible Settings: **D4, ESF** Default Setting: **ESF**
Specifies the framing format for transmitted and received signals on the T1 network interface. **D4** – Uses D4 framing format. NOTE: This setting is not recommended by network carriers. False yellow alarms may occur after traffic has been running and the channel returns to idle, or when there is light traffic when other settings are selected. ESF format does not create this problem. **ESF** – Uses Extended Superframe framing format.
Line Coding Format
Possible Settings: **AMI, B8ZS** Default Setting: **B8ZS**
Specifies the line coding format for the network interface. **AMI** – Uses Alternate Mark Inversion (AMI) line coding format. **B8ZS** – Uses Bipolar 8 Zero Substitution (B8ZS) line coding format.
Line Build Out (LBO)
Possible Settings: **0.0, –7.5, –15, –22.5** Default Setting: **0.0**
Specifies the line build out for the signal transmitted to the network. **0.0, –7.5, –15, –22.5** – Specifies line build out in dB.

Table 3-2. Network Physical Interface Options (2 of 3)

Network Initiated LLB
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Allows the initiation and termination of the line loopback (LLB) to be controlled by the receipt of LLB-Actuate and LLB-Release commands from the network. **Enable** – LLB is controlled by LLB-Actuate and LLB-Release commands. Receiving a LLB-Actuate command causes the DSU/CSU to enter a line loopback (provided an LLB can be performed in the DSU/CSU's current state). Receiving an LLB-Release command terminates the LLB. **Disable** – The DSU/CSU ignores the LLB-Actuate and LLB-Release commands. NOTE: When disabled, the system is not in compliance with ANSI T1.403 or AT&T TR 62411.
Network Initiated PLB
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Allows the initiation and termination of the payload loopback (PLB) to be controlled by the receipt of PLB-Actuate and PLB-Release commands from the network. *Display Conditions* – This option only appears when Line Framing Format is set to ESF. **Enable** – PLB is controlled by PLB-Actuate and PLB-Release commands. Receiving a PLB-Actuate command causes the system to enter a payload loopback (provided a PLB can be performed in the unit's current state). Receiving a PLB-Release command terminates the PLB. **Disable** – The DSU/CSU ignores the PLB-Actuate and PLB-Release commands. NOTE: When disabled, the unit is not in compliance with ANSI T1.403 or AT&T TR 54016.
ANSI Performance Report Messages
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether ANSI T1.403 compliance performance report messages (PRMs) are generated and sent to the network over the ESF facility data link every second. *Display Conditions* – This option only appears when Line Framing Format is set to ESF. **Enable** – Generates and sends PRMs. **Disable** – Does not generate and send PRMs.

Table 3-2. Network Physical Interface Options (3 of 3)

Excessive Error Rate Threshold
Possible Settings: **10E-4, 10E-5, 10E-6, 10E-7, 10E-8, 10E-9** Default Setting: **10E-4**
Sets the error rate threshold that determines when an EER condition is declared. The excessive error rate is determined by the ratio of the number of CRC6 errors to the total number of bits received over a set period of time. *Display Conditions* – This option only appears when Line Framing Format is set to ESF. **10E-4** – Declares an EER if more than 1,535 CRC6 errors are detected in a 10-second period. Clears when fewer than 1,536 CRC6 errors are detected within the same time period. **10E-5** – Declares an EER if more than 921 CRC6 errors are detected in a 60-second period or a 10^{-4} condition occurs. Clears when fewer than 922 CRC6 errors are detected within the same time period. **10E-6** – Declares an EER if more than 92 CRC6 errors are detected in a 60-second period or a 10^{-5} or 10^{-4} condition occurs. Clears when fewer than 93 CRC6 errors are detected within the same time period. **10E-7** – Declares an EER if more than 9 CRC6 errors are detected in a 60-second period or a 10^{-6}, or 10^{-5}, or 10^{-4} condition occurs. Clears when fewer than 10 CRC6 errors are detected within the same time period. **10E-8** – Declares an EER if more than 41 CRC6 errors are detected in three 15-minute intervals or a 10^{-7}, 10^{-6}, 10^{-5}, 10^{-4} condition occurs. Clears when fewer than 42 CRC6 errors are detected within the same time period. **10E-9** – Declares an EER if more than 4 CRC6 errors are detected in three 15-minute intervals or a 10^{-8}, 10^{-7}, 10^{-6}, 10^{-5}, or 10^{-4} condition occurs. Clears when fewer than 5 CRC6 errors are detected within the same time period.
Circuit Identifier
Possible Settings: ***Text Field*, Clear** Default Setting: **blank**
Identifies the transmission vendor's circuit information to facilitate troubleshooting. ***Text Field*** – Edit or display circuit identifier information (maximum 255 characters). **Clear** – Removes the circuit identifier information.

Configuring the User Data Port

Select Physical from the Data Ports menu to configure the physical characteristics for the user data port (see Table 3-3, Data Port Physical Interface Options).

Main Menu → Configuration → Data Ports → Physical

Table 3-3. Data Port Physical Interface Options (1 of 3)

Port Base Rate
Possible Settings: **Nx64, Nx56** Default Setting: **Nx64**
Determines the base rate of the data port. The actual data rate is a multiple (from 1 to 24 times) this base rate. **Nx64** – The port base rate is 64 Kbps. **Nx56** – The port base rate is 56 Kbps.
Invert Transmit Clock
Possible Settings: **Auto, Enable, Disable** Default Setting: **Auto**
Determines whether the clock supplied by the DSU/CSU on interchange circuit DB (ITU 114) – Transmit Signal Element Timing (DCE Source) TXC is phase inverted with respect to the clock used to time the incoming Transmitted Data (TD). **Auto** – The port will check the clock supplied by the DCE on TXC on this port. If necessary, the port will automatically phase invert the clock with respect to the transmitted data. **Enable** – Phase inverts the TXC clock. Use this setting when long cable lengths between the DSU/CSU and the DTE are causing data errors. **Disable** – Does not phase invert the TXC clock.
Transmit Clock Source
Possible Settings: **Internal, External** Default Setting: **Internal**
Determines whether the DTE's transmitted data is clocked into the DSU/CSU by its internal transmit clock or by the external clock provided by the DTE. NOTE: Changing settings for this configuration option causes the DSU/CSU to abort any physical port tests, including any DTE-initiated loopback tests. **Internal** – The DSU/CSU uses the interchange circuit DB (ITU 114) – Transmit Signal Element Timing (TXC) (DCE source) for timing the incoming data. **External** – The DTE provides the clock for the transmitted data, and the DSU/CSU uses the interchange circuit DA (ITU 113) – Transmit Signal Element Timing (XTXC) (DTE source) for timing the incoming data.

Table 3-3. Data Port Physical Interface Options (2 of 3)

Monitor RTS (Control)
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether the state of the Request To Send (RTS) circuits on the user data port will be used to determine when valid data communication is possible with the DTE. When the RTS off condition is detected, CTS is deasserted. **Enable** – Interchange circuit CA (ITU 105) – RTS is monitored to determine when valid data communication is possible with the DTE. **Disable** – RTS is not monitored. RTS is assumed to be asserted and data is being transmitted, regardless of the state of the lead.
Monitor DTR
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether the state of the DTE Ready (DTR) circuit on the user data port will be used to determine when valid data communication is possible with the DTE. When the DTR off condition is detected, an alarm is generated. **Enable** – Interchange circuit CD (ITU 108/1/2) – DTR is monitored to determine when valid data is sent from the DTE. **Disable** – DTR is not monitored. DTR is assumed to be asserted and data is being transmitted, regardless of the state of the lead.
Port (DTE) Initiated Loopbacks
Possible Settings: **Local**, **Disable** Default Setting: **Disable**
Allows a local external DTE Loopback to be started or stopped via the port's attached data terminal equipment using the port's interchange lead LL (ITU 141). **Local** – The DTE attached to the port controls the local external DTE Loopback. **Disable** – The DTE attached to the port cannot control the local external DTE Loopback.

Table 3-3. Data Port Physical Interface Options (3 of 3)

Network Initiated Data Channel Loopback
Possible Settings: **Disable, V.54, ANSI_FT1, V.54_&_ANSI** Default Setting: **Disable**
Allows the initiation and termination of the Data Channel Loopback (DCLB V.54 Loop 2) to be controlled by the receipt of a DCLB-actuate or DCLB-release sequence (either V.54 or FT1-ANSI compliant) from the network on the DS0s used for the network link. When enabled and a DCLB-activate sequence is received, the unit initiates a DCLB on the network interface. When a DCLB-release sequence is received, the DCLB is stopped. **Disable** – DCLB-actuate and DCLB-release sequences are ignored. **ANSI_FT1** – DCLB-actuate and DCLB-release sequences compliant with the ANSI T1.403, Annex B standard are recognized and control initiation and termination of a DCLB for the network link. **V.54_&_ANSI** – DCLB-actuate and DCLB-release sequences that comply with either V.54 or ANSI T1.403, Annex B standard are recognized and control initiation and termination of a DCLB for the network link. The actuate and release sequences do not need to match (for example, a DCLB started with a V.54 actuate sequence can be stopped with an FT1 release sequence).

Assigning Time Slots/Cross Connections

The Time Slot Assignment/Cross Connect feature provides an easy method of creating cross-connections to the synchronous data interface. The system allows you to assign DS0s on the T1 network interface and between the user data port and network interface in order to share the T1 network.

You can also clear cross-connection assignments for the unit, or for a selected interface.

NOTE:

Although it is not required, progressing through each screen in order, from top to bottom, helps to minimize errors.

Use the following procedures to assign cross connections.

Assigning the Synchronous Data Port to Network Time Slots

Use the Sync Data Port Assignment screen to assign the synchronous data port to network interface time slots. Follow this menu sequence:

Main Menu → *Configuration* → *Time Slot Assignment* → *Sync Data Port Assignments* or

Synchronous Data Port Assignment Screen Example

```
main/config/tslot_assign/sync_data/net                                  7123
Device Name: Node A                                        09/09/2001 03:02

                        SYNC DATA PORT ASSIGNMENT

                           Assign To: Net1

   N01       N02       N03       N04       N05       N06       N07       N08
Available Available Available Available Available  Port-1    Port-1   Available

   N09       N10       N11       N12       N13       N14       N15       N16
Available Available Available Available Available Port-1    Port-1    Available

   N17       N18       N19       N20       N21       N22       N23       N24
Available Available Available Available Available Available Available Available1




--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
 Save                       ClearAll
```

Value	Meaning
Assign To	Specifies Net1 (network) time slots.
N*tt*	This field represents time slot *tt* of the network interface.
Available	The time slot is currently unassigned.
Port-1	Synchronous data Port-1 is assigned to the time slot.

▶ Procedure

1. Select the following menu selection sequence:

   Main Menu → *Configuration* → *Time Slot Assignment* → *Sync Data Port Assignments* or

2. Select an interface in the Assign To field. A matrix of the current cross-connect status of all time slots on the selected interface appears.
3. Move the cursor to the next time slot that can be edited (underlined). Use the spacebar or type in the desired time slot to display its time slot assignment.
4. Repeat Step 3 until the synchronous data port is assigned to all desired time slots.
5. Save the configuration.

Clearing Assignments

Clearing assignments sets all time slots to **Unassgn** (unassigned).

Main Menu → *Configuration* → *Time Slot Assignment* → *Clear Assignments*

Setting Up Management and Communication Options

The following sections explain options that can be selected from the Management and Communication menu:

- *Configuring Node IP Information*
- *Configuring General SNMP Management*
- *Configuring Telnet and/or FTP Session Support*
- *Configuring SNMP NMS Security*
- *Configuring SNMP Traps*
- *Configuring the Ethernet Port*
- *Configuring the Communication Port*
- *Configuring the COM Port to Support an External Modem*

Configuring Node IP Information

Select Node IP to display, add, or change the information necessary to support general IP communications for the node (see Table 3-4, Node IP Options). When deploying units to remote sites, minimally configure the Node IP Address and Subnet Mask.

Main Menu → Configuration → Management and Communication → Node IP

Table 3-4. Node IP Options (1 of 2)

Node IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address needed to access the node. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the node, which can be viewed or edited. **Clear** – Fills the node IP address with zeros.
Node Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the subnet mask associated with the IP address that is needed to access the node. **000.000.000.000 – 255.255.255.255** – Shows the subnet mask for the node, which can be viewed or edited. **Clear** – Fills the node subnet mask with zeros. When the node's subnet mask is all zeros, the IP protocol creates a default subnet mask based upon the class of the IP address: Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000.

Table 3-4. Node IP Options (2 of 2)

Default IP Destination
Possible Settings: **None, COM, Ethernet** Default Setting: **None**
Specifies an IP destination to route data that does not have a specifically defined route. **None** – No default network destination is specified. Unrouteable data will be discarded. This is the recommended setting. **COM** – Specifies that the default destination is connected to the COM port. Only appears when Port Use is set to Net Link (see Table 3-10, Communication Port Options). **Ethernet** – Specifies that the default destination is connected to the Ethernet port. Only appears when the Ethernet port's Interface Status option is enabled. When selected, the Default Gateway Address must also be configured (see Table 3-9, Ethernet Management Options).

Configuring General SNMP Management

Select General SNMP Management to add, change, or delete the information needed to allow the DSU/CSU to be managed as an SNMP agent by the NMS supporting the SNMP protocols (see Table 3-5, General SNMP Management Options).

Main Menu → Configuration → Management and Communication → General SNMP Management

You must have Level-1 access to display or configure these options.

Table 3-5. General SNMP Management Options (1 of 2)

SNMP Management
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the DSU/CSU can be managed as an SNMP agent by an SNMP-compatible NMS. **Enable** – Can be managed as an SNMP agent. **Disable** – Cannot be managed as an SNMP agent. The DSU/CSU will not respond to SNMP messages nor send SNMP traps.
Community Name 1
Possible Settings: ***ASCII text entry*, Clear** Default Setting: **Public** in ASCII text field
Specifies the first of two names that are allowed to access the objects in the DSU/CSU's MIB. The community name must be supplied by an external SNMP manager whenever the manager tries to access an object in the MIB. ***ASCII text entry*** – Adds to or changes Community Name 1 (maximum 255 characters). **Clear** – Clears Community Name 1.
Name 1 Access
Possible Settings: **Read, Read/Write** Default Setting: **Read/Write**
Specifies the type of access allowed to the objects in the MIB. This is the type of access allowed for external SNMP managers accessing MIB objects using Community Name 1. **Read** – Allows read-only access (SNMP Get command). This includes all objects specified as either read-only or read/write in the MIB RFCs. **Read/Write** – Allows read and write access (SNMP **get** and **set** commands).
Community Name 2
Possible Settings: ***ASCII text entry*, Clear** Default Setting: **Clear**
Specifies the second of two names that are allowed to access the objects in the DSU/CSU's MIB. The community name must be supplied by an external SNMP manager whenever the manager tries to access an object in the MIB. ***ASCII text entry*** – Adds to or changes Community Name 2 (maximum 255 characters). **Clear** – Clears Community Name 2.

Table 3-5. General SNMP Management Options (2 of 2)

Name 2 Access
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Specifies the type of access allowed to the objects in the MIB. This is the type of access allowed for external SNMP managers accessing MIB objects using Community Name 2. **Read** – Allows read-only access (SNMP Get command). This includes all objects specified as either read-only or read/write in the MIB RFCs. **Read/Write** – Allows read and write access (SNMP **get** and **set** commands).

Configuring Telnet and/or FTP Session Support

Telnet and FTP options control whether a Telnet or FTP (File Transport Protocol) session is allowed through an interconnected IP network and the access security applicable to the session. Two Telnet sessions can be active at a time (see Table 3-6, Telnet and FTP Session Options).

Main Menu → Configuration → Management and Communication → Telnet and FTP Session

Table 3-6. Telnet and FTP Session Options (1 of 3)

Telnet Session
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether the DSU/CSU will respond to a session request from a Telnet client on an interconnected IP network. **Enable** – Allows Telnet sessions between the DSU/CSU and Telnet client. **Disable** – Does not allow Telnet sessions.
Telnet Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether a user ID and password (referred to as the login) are required to access the menu-driven user interface via a Telnet session. If required, the login used is the same login used for an menu-driven user interface session. **Enable** – Requires a login to access a Telnet session. **Disable** – Does not require a login.

Table 3-6. Telnet and FTP Session Options (2 of 3)

Session Access Level
Possible Settings: **Level-1, Level-2, Level-3** Default Setting: **Level-1**
Specifies the highest security level allowed when accessing the menu-driven user interface via a Telnet session. If a login is required for the session, the effective access level is also determined by the user's access level. When a login is *not* required, the effective access level is determined by this option. NOTE: The effective access level is always the lowest one assigned to either the session or the user. For example, if the assigned Session Access Level is Level-2, but the User Access Level is Level-3, then only level-3 access is allowed for the session. **Level-1** – Allows Telnet access by users with Login ID access levels of 1, 2, and 3, with the capability to view system information, change configuration options, and run tests. This is the highest access level allowed. CAUTION: Before changing the session access level to Level-2 or 3, make sure that the COM port's Port Access Level is set to Level-1 and that at least one Login ID is set to Level-1. Otherwise, access will be lost. If this occurs, you must reset the unit to the factory defaults and begin the configuration process again. A reset is required if the Communication Port's Port Use option is set to Net Link (see Table 3-1, General System Options). **Level-2** – Allows Telnet access by users with Login ID access levels of 1, 2, and 3, with the capability to view system information and run tests only; they cannot change configuration options. **Level-3** – Allows Telnet access by users with Login ID access levels of 1, 2, and 3, with the capability to view system information only; they cannot change configuration options or run tests.
Inactivity Timeout
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether a Telnet session is disconnected after a specified period of keyboard inactivity. **Enable** – Terminates the session after the Disconnect Time expires. **Disable** – Does not terminate Telnet session during inactivity.
Disconnect Time (Minutes)
Possible Settings: **1 – 60** Default Setting: **10**
Sets the amount of keyboard inactive time allowed before a user session is disconnected. *Display Conditions* – This option does not appear when Inactivity Timeout is disabled. **1 – 60** – Up to an hour can be set.

Table 3-6. Telnet and FTP Session Options (3 of 3)

FTP Session
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the system responds as a server when an FTP (file transfer protocol) client on an interconnected IP network requests an FTP session. This option must be enabled when downloading files. **Enable** – Allows an FTP session between the system and an FTP client. **Disable** – Does not allow FTP sessions.
FTP Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether a login ID and password are required for an FTP session. If required, the login used is the same login used for a menu-driven user interface session. **Enable** – User is prompted for a login ID and password. **Disable** – No login is required for an FTP session.

Configuring SNMP NMS Security

Select SNMP NMS Security from the Management and Communication menu to display, add, or change SNMP security configuration options for the DSU/CSU to set up trap managers (see Table 3-7, SNMP NMS Security Options).

Main Menu → Configuration → Management and Communication → SNMP NMS Security

A table is displayed consisting of the network management systems identified by IP address that are allowed to access the DSU/CSU by SNMP.

Table 3-7. SNMP NMS Security Options (1 of 2)

NMS IP Validation
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether security checks are performed on the IP address of SNMP management systems attempting to access the node. Only allows access when the sending manager's IP address is listed on the SNMP NMS Security Options screen. **Enable** – Performs security checks. **Disable** – Does not perform security checks.
Number of Managers
Possible Settings: **1 – 10** Default Setting: **1**
Specifies the number of SNMP management systems that are authorized to send SNMP messages to the DSU/CSU. An IP address must be configured for each management system allowed to send messages. Configure IP addresses in the NMS *n* IP Address configuration option. **1 – 10** – Specifies the number of authorized SNMP managers.
NMS *n* IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Provides the IP address of an SNMP manager that is authorized to send SNMP messages to the unit. If an SNMP message is received from an unauthorized NMS and its IP address cannot be matched here, access is denied and an authenticationFailure trap is generated. If a match is found, the type of access (read-only or read/write) is determined by the corresponding Access Type. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **001.000.000.000 – 223.255.255.255** – Adds to or changes the NMS IP address. **Clear** – Fills the NMS IP address with zeros.

Table 3-7. SNMP NMS Security Options (2 of 2)

Access Type
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Specifies the type of access allowed for an authorized NMS when IP address validation is performed. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **Read** – Allows read-only access (SNMP Get command) to the MIB objects. This includes all objects specified as either read-only or read/write in the MIB RFCs. **Read/Write** – Allows read and write access (SNMP Get and Set commands) to the MIB objects. However, access for all read-only objects is specified as read-only.

Configuring SNMP Traps

Select SNMP Traps from the Management and Communication menu to configure SNMP traps when a trap is generated (see Table 3-8, SNMP Traps Options).

Main Menu → Configuration → Management and Communication → SNMP Traps

- See Appendix B, *SNMP MIBs and Traps*, for trap format standards and special trap features.

Table 3-8. SNMP Traps Options (1 of 3)

SNMP Traps
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether the DSU/CSU sends trap messages to the currently configured SNMP trap manager(s). **Enable** – Sends trap messages. **Disable** – Does not send trap messages.
Number of Trap Managers
Possible Settings: **1 – 6** Default Setting: **1**
Specifies the number of SNMP management systems that will receive SNMP trap messages from the DSU/CSU. An NMS IP Address must be configured in the NMS *n* IP Address configuration option for each trap manager to receive trap messages. **1 – 6** – Specifies the number of trap managers.
NMS *n* IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address that identifies the SNMP manager(s) to receive SNMP traps. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **001.000.000.000 – 223.255.255.255** – Adds to or changes the IP address for the trap manager. **Clear** – Fills the NMS IP address with zeros.

Table 3-8. SNMP Traps Options (2 of 3)

Initial Route Destination
Possible Settings: **AutoRoute, Ethernet, COM** Default Setting: **AutoRoute**
Specifies the initial route used to reach the specified Trap Manager. When proprietary RIP is active, only one unit in the network needs to specify an interface as the initial destination. All other units can use the default setting. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **AutoRoute** – Uses proprietary RIP from other DSU/CSUs to learn the route for sending traps to the specified Trap Manager, or the Default IP Destination when no route is available in the routing table (see Table 3-4, Node IP Options). **Ethernet** – Uses the Ethernet port. Only appears when the Ethernet port's Interface Status option is enabled (see Table 3-9, Ethernet Management Options). **COM** – Uses the COM port. Only available when Port Use is set to Net Link (see Table 3-10, Communication Port Options).
General Traps
Possible Settings: **Disable, Warm, AuthFail, Both** Default Setting: **Both**
Determines whether SNMP trap messages for warmStart and/or authenticationFailure events are sent to the currently configured trap manager(s). **Disable** – Does not send trap messages for these events. **Warm** – Sends trap messages for warmStart events only. **AuthFail** – Sends trap messages for authenticationFailure events only. **Both** – Sends trap messages for both warmStart and authenticationFailure events.
Enterprise Specific Traps
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether trap messages for enterpriseSpecific events are sent to the currently configured trap manager(s). **Enable** – Sends trap messages for enterpriseSpecific events. **Disable** – Does not send trap messages for enterpriseSpecific events.
Link Traps
Possible Settings: **Disable, Up, Down, Both** Default Setting: **Both**
Determines whether SNMP linkDown or linkUp traps are sent to the currently configured trap manager(s). A linkDown trap indicates that the unit recognizes a failure in one of the interfaces. A linkUp trap indicates that the unit recognizes that one of its interfaces is active. Use the Link Traps Interface and the DLCI Traps on Interface configuration options to specify which interface will monitor linkUp and linkDown traps messages. **Disable** – Does not send linkDown or linkUp trap messages. **Up** – Sends trap messages for linkUp events only. **Down** – Sends trap messages for linkDown events only. **Both** – Sends trap messages for linkUp and linkDown events.

Table 3-8. SNMP Traps Options (3 of 3)

Link Traps Interfaces
Possible Settings: **Network, T1s, Ports, All** Default Setting: **All**
Specifies which interfaces will generate linkUp, linkDown, and enterpriseSpecific trap messages. These traps are not supported on the COM port. **Network** – Generates these trap messages on the network interface only. **T1s** – For applicable T1 DSU/CSUs, generates these trap messages for linkUp, linkDown, and enterpriseSpecific events on both the T1 network and DSX-1 interfaces. **Ports** – Generates these trap messages for linkUp, linkDown, and enterpriseSpecific events on the user data port only. **All** – Generates these trap messages for linkUp and enterpriseSpecific events on all interfaces, except for the COM port, that are applicable to the model.

Configuring the Ethernet Port

Select Ethernet Management from the Management and Communication menu to configure the Ethernet port (see Table 3-9, Ethernet Management Options).

Main Menu → Configuration → Management and Communication → Ethernet Management

Table 3-9. Ethernet Management Options (1 of 2)

Interface Status
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether the Ethernet port is being used and can be configured. **Enable** – The port is active. It can receive Version 2 or IEEE 802.3 MAC frames, or transmit Version 2 MAC frames only. When the Ethernet port is enabled, the **`Would you like to set the Node's IP Destination to Ethernet?`** prompt is displayed. ■ If you select Yes, the Default IP Destination (see Table 3-4, Node IP Options) is automatically changed to Ethernet, so the Ethernet port's Default Gateway Address is used for packets that do not have a route. This is required when the NMS is on a different subnet than the unit. ■ If you select No, the COM port will be used for packets without a route. **Disable** – The port is not active. When the port is disabled, the following will occur: ■ No alarms or traps configured for the port will be generated. ■ All port uses that refer to the Ethernet port, like the Default IP Destination and Initial Route Destination, will be reset to their default values (see Table 3-4, Node IP Options, and Table 3-8, SNMP Traps Options).
IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address needed to access the Ethernet port. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the port, which can be viewed or edited. **Clear** – Fills the IP address with zeros.
Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the subnet mask associated with the IP address that is needed to access the Ethernet port. **000.000.000.000 – 255.255.255.255** – Set the Ethernet port's subnet mask. The range for each byte is 000 to 255. **Clear** – Fills the subnet mask associated with the IP address with zeros.

Table 3-9. Ethernet Management Options (2 of 2)

Default Gateway Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address for the port's default gateway. It is used for packets that do not have a route. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the port, which can be viewed or edited (i.e., a router on the LAN). **Clear** – Fills the default gateway's IP address with zeros.

Configuring the Communication Port

Select Communication Port from the Management and Communication menu to display or change the communication port configuration options (see Table 3-10, Communication Port Options).

Main Menu→ Configuration→ Management and Communication→ Communication Port

Table 3-10. Communication Port Options (1 of 4)

Port Use
Possible Settings: **Terminal, Net Link** Default Setting: **Terminal**
Assigns a specific use to the COM port. NOTE: If the Default IP Destination is set to COM (see Table 3-4, Node IP Options) and you change Port Use to Terminal, the Default IP Destination is forced to None. **Terminal** – The COM port is used for the asynchronous terminal connection. **Net Link** – The COM port is the network communications link to the IP network or IP device port.
Data Rate (Kbps)
Possible Settings: **9.6, 14.4, 19.2, 28.8, 38.4, 57.6, 115.2** Default Setting: **19.2**
Specifies the rate for the COM port in kilobits per second. **9.6 – 115.2 Kbps** – Sets the communication port speed.
Character Length
Possible Settings: **7, 8** Default Setting: **8**
Specifies the number of bits needed to represent one character. NOTE: Character length defaults to 8 and cannot be changed if Port Use is set to Net Link. **7** – Sets the character length to seven bits. **8** – Sets the character length to eight bits. Use this setting if using the COM port as the network communication link.
Parity
Possible Settings: **None, Even, Odd** Default Setting: **None**
Provides a method of checking the accuracy of binary numbers for the COM port. A parity bit is added to the data to make the “1” bits of each character add up to either an odd or even number. Each character of transmitted data is approved as error-free if the “1” bits add up to an odd or even number as specified by this configuration option. **None** – Provides no parity. **Even** – Makes the sum of all 1 bits and its corresponding parity bit always even. **Odd** – Makes the sum of all 1 bits and its corresponding parity bit always odd.

Table 3-10. Communication Port Options (2 of 4)

Stop Bits
Possible Settings: **1, 2** Default Setting: **1**
Determines the number of stop bits used for the COM port. **1** – Provides one stop bit. **2** – Provides two stop bits.
Ignore Control Leads
Possible Settings: **Disable, DTR** Default Setting: **Disable**
Specifies whether DTR is used. **Disable** – Treats control leads as standard operation. **DTR** – Ignores DTR. This may be necessary when connecting to some PAD devices.
Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether a user ID and password (referred to as the login) is required in order to log on to the asynchronous terminal connected to the COM port. *Display Conditions* – This option only appears when Port Use is set to Terminal. **Enable** – Requires a login to access the menu-driven user interface. **Disable** – Does not requires a login.
Port Access Level
Possible Settings: **Level-1, Level-2, Level-3** Default Setting: **Level-1**
Specifies level of user access privilege for an asynchronous terminal connected to the COM port. If a login is required for the port, the effective access level is determined by the user's access level. When a login is *not* required, the effective access level is determined by this option. NOTE: The effective access level is always the lowest one assigned to either the port or the user. For example, if the Port Access Level assigned is Level-2, but the User Access Level is Level-3, then only level-3 access will be permitted for the port. *Display Conditions* – This option only appears when Port Use is set to Terminal. **Level-1** – Allows full access and control of the device including monitoring, diagnostics, and configuration. The user can add, change, and display configuration options, and perform device testing. CAUTION: Before changing the communication port's access level to Level-2 or 3, make sure that the Telnet Session Access Level is set top Level-1 and at least one Login ID is set to Level-1. Otherwise, access will be lost. If this occurs, you must reset the unit to the factory defaults and begin the configuration process again. **Level-2** – Allows limited access and control of the device. The user can monitor and perform diagnostics, display status and configuration option information. **Level-3** – Allows limited access with monitoring control only. The user can monitor and display status and configuration screens only.

Table 3-10. Communication Port Options (3 of 4)

Inactivity Timeout
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether a user session is disconnected after a specified time of inactivity (no keyboard activity). *Display Conditions* – This option only appears when Port Use is set to Terminal. **Enable** – Disconnects user session after the specified time of inactivity. **Disable** – Does not disconnect user session.
Disconnect Time (Minutes)
Possible Settings: **1 – 60** Default Setting: **10**
Specifies the number of minutes of inactivity that can elapse before the session is disconnected. *Display Conditions* – This option only appears when Port Use is set to Terminal. **1 – 60** – Sets the time from 1 to 60 minutes (inclusive).
IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies a unique IP address for accessing the unit via the COM port. This option is only in effect when the COM port is configured as a network communication link (Port Use option is set to Net Link). *Display Conditions* – This option only appears when Port Use is set to Net Link. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the COM port, which you can view or edit. **Clear** – Clears the IP address for the COM port and fills the address with zeros. When the IP Address is all zeros, the COM port uses the Node IP Address if one has been configured.
Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the subnet mask needed to access the unit. Only in effect when the COM port is configured as a network communication link (Port Use option is set to Net Link). *Display Conditions* – This option only appears when Port Use is set to Net Link. **000.000.000.000 – 255.255.255.255** – Shows COM port subnet mask, which you can view or edit. **Clear** – Clears the subnet mask for the COM port and fills the address with zeros. When the node subnet mask is all zeros, the IP protocol creates a default subnet mask based upon the IP address class: Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000.

Table 3-10. Communication Port Options (4 of 4)

RIP
Possible Settings: **None, Standard_out** Default Setting: **None**
Specifies which Routing Information Protocol (RIP) is used to enable routing of management data between devices. *Display Conditions* – This option only appears when Port Use is set to Net Link. **None** – No routing is used. **Standard_out** – The device will send standard RIP messages to communicate routing information about other FrameSaver units in the network. Standard RIP messages received on this link are ignored. NOTE: The router must be configured to receive RIP on the port connected to the COM port, configured as the management interface. To create this management interface, make sure that Node or COM Port IP information has been set up (refer to *Configuring Node IP Information* on page 3-19).

Configuring the COM Port to Support an External Modem

Select External Modem (Com Port) to display or change the configuration options that control call processing for an external device attached to the COM port (see Table 3-11, External Modem (COM Port) Options).

Main Menu → Configuration → Management and Communication → External Modem (Com Port)

NOTE:

A standard EIA-232 crossover cable is required when connecting an external modem to the DSU/CSU's COM port. See *Standard EIA-232-D Crossover Cable* in Appendix C, *Connectors, Cables, and Pin Assignments*, for cable pin assignments.

Table 3-11. External Modem (COM Port) Options

External Modem Commands
Possible Settings: **Disable, AT** Default Setting: **Disable**
Specifies the type of commands to be sent over the COM port. **Disable** – Commands will not be sent over the COM port. **AT** – Standard Attention (AT) Commands are sent over the COM port to control the external device. All AT command strings will end with a carriage return (hex 0x0D) and a line feed (hex 0x0A). CAUTION: Do *not* use this setting if you have an asynchronous terminal connected to the COM port.
Dial-In Access
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Controls whether external devices can dial-in to the DSU/CSU through the COM port (based on the Port Use option setting). *Display Conditions* – This option does not appear if External Modem Commands is disabled. **Enable** – Answers incoming calls and establishes connection to the remote terminal or IP network. **Disable** – Does not answer incoming calls.

Security and Logins

4

This chapter includes the following:

- *Limiting Access* on page 4-2
- *Controlling Asynchronous Terminal Access* on page 4-2
- *Controlling External COM Port Device Access* on page 4-4
- *Controlling Telnet or FTP Access* on page 4-4
  - *Limiting Telnet Access*
  - *Limiting FTP Access*
- *Controlling SNMP Access* on page 4-7
  - *Disabling SNMP Access*
  - *Assigning SNMP Community Names and Access Levels*
  - *Limiting SNMP Access through IP Addresses*
- *Creating a Login* on page 4-10
- *Modifying a Login* on page 4-11
- *Deleting a Login* on page 4-11

Limiting Access

The 7123 SNMP DSU/CSU provides access security on the following interfaces:

- Asynchronous (async) terminal
- Telnet
- FTP
- SNMP

Up to two direct or Telnet sessions can be active at any given time; that is, you can have two simultaneous Telnet sessions, or one Telnet session and one active asynchronous terminal session, or two simultaneous asynchronous terminal sessions.

Controlling Asynchronous Terminal Access

Direct asynchronous terminal access to the menu-driven user interface can be limited by:

- Requiring a login.
- Assigning an access level to the port or interface.

See *Configuring the Communication Port* in Chapter 3, *Configuration,* for more information about communication (COM) port configuration options.

▶ Procedure

To limit asynchronous terminal access to the menu-driven user interface:

1. Select the Communication Port options.

   Main Menu → Configuration → Management and Communication → Communication Port

2. Set the following configuration options, as appropriate.

To . . .	Set the configuration option . . .
Require a login	Login Required to Enable. **NOTE:** User ID and password combinations must be defined. See *Creating a Login* on page 4-10.
Limit the effective access level to Level-3 or Level-2	Port Access Level to Level-2 or Level-3. **NOTE:** Regardless of a user's login access level, a user cannot operate at a level higher than the access level specified for the port (e.g., if a user has a Level-1 login and Level-2 port access has been set, the Level-1 user can only operate as a Level-2 user). If you are going to allow Level-1 users to configure the unit, keep the access at Level-1.

NOTE:

Should you be locked out inadvertently, see *Resetting the Unit and Restoring Communication* in Chapter 6, *Troubleshooting*.

3. Save your changes.

Controlling External COM Port Device Access

Dial-in access can be controlled when an external device (modem) is connected to the unit's communication (COM) port. The External Device Commands option must be set to AT.

▶ Procedure

To control dial-in access:

1. Select the External Modem options.

   Main Menu → Configuration → Management and Communication → External Modem (Com Port)

2. Enable the Dial-In Access configuration option.

   This option only appears when the External Device Commands option is set to AT.

3. Save your change.

See *Configuring the COM Port to Support an External Modem* in Chapter 3, *Configuration,* for more information about external device communication port configuration options.

Controlling Telnet or FTP Access

The DSU/CSU provides several methods for limiting access via a Telnet or FTP session. Telnet or FTP access can be on a standard management link or on a service provider's troubleshooting (TS) management link.

Limiting Telnet Access

Telnet access can be limited by:

- Disabling Telnet access completely.
- Requiring a login for Telnet sessions.
- Assigning an access level for Telnet sessions.

▶ Procedure

To limit Telnet access:

1. Select the Telnet and FTP Session options.

   Main Menu → Configuration → Management and Communication → Telnet and FTP Sessions

2. Set the following configuration options, as appropriate.

To . . .	Set the configuration option . . .
Disable Telnet access	Telnet Session to Disable.
Require a login	Login Required to Enable. **NOTE:** User ID and password combinations must be defined. See *Creating a Login* in Chapter 4, *Security and Logins*.
Assign an access level	Session Access Level to Level-2 or Level-3. **NOTE:** Regardless of a user's login access level, a user cannot operate at a level higher than the access level specified for the Telnet session (e.g., if a user has a Level-1 login and Level-2 telnet access has been set, the Level-1 user can only operate as a Level-2 user). If you are going to allow users to configure the unit, keep the access at Level-1.

3. Save your changes.

See *Configuring Telnet and/or FTP Session Support* in Chapter 3, *Configuration,* for more information about setting Telnet configuration options.

Limiting FTP Access

FTP access can be limited by:

- Disabling FTP access completely.
- Requiring a user ID and password to login.

▶ Procedure

To limit FTP access:

1. Select the Telnet and FTP Session options.

   Main Menu → Configuration → Management and Communication → Telnet and FTP Sessions

2. Set the following configuration options, as appropriate.

To . . .	Set the configuration option . . .
Disable FTP	FTP Session to Disable.
Require a login	Login Required to Enable. **NOTE:** User ID and password combinations must be defined. See *Creating a Login* on page 4-10. If you want to allow users to configure the unit or perform file transfers, including downloads, keep the access at Level-1. Level-1 access is required to download software to the unit, or to upload or download configuration files. Level-3 is sufficient for NMS access for SLV historical information.

3. Save your changes.

See *Configuring Telnet and/or FTP Session Support* in Chapter 3, *Configuration,* for more information about setting FTP configuration options.

Controlling SNMP Access

The DSU/CSU supports SNMP Version 1, which provides limited security through the use of community names. There are three methods for limiting SNMP access:

- Disabling SNMP access.
- Assigning SNMP community names and the access type.
- Assigning IP addresses of those NMSs that can access the unit.

Disabling SNMP Access

When the SNMP access is disabled, the DSU/CSU will not respond to SNMP messages.

▶ Procedure

To disable SNMP access:

1. Select the General SNMP Management options.

   Main Menu → Configuration → Management and Communication → General SNMP Management

2. Disable the SNMP Management option.
3. Save your change.

See *Configuring General SNMP Management* in Chapter 3, *Configuration,* for more information about General SNMP Management configuration options.

Assigning SNMP Community Names and Access Levels

The DSU/CSU supports the SNMP protocol and can be managed by an SNMP manager. SNMP manager access can be limited by:

- Assigning the SNMP community names that are allowed to access the DSU/CSU's Management Information Base (MIB).
- Specifying the type of access allowed for each SNMP community name.

Whenever an SNMP manager attempts to access an object in the MIB, the community name must be supplied.

▶ Procedure

To assign SNMP community names and access types:

1. Select the General SNMP Management options.

   Main Menu → Configuration → Management and Communication → General SNMP Management

2. Set the following configuration options, as appropriate.

To . . .	Set the configuration option . . .
Assign SNMP community names	Community Name 1 and Community Name 2 to a community name text, up to 255 characters in length.
Assign the type of access allowed for the SNMP community names	Name 1 Access and Name 2 Access to Read or Read/Write.

3. Save your changes.

See *Configuring General SNMP Management* in Chapter 3, *Configuration,* for more information about General SNMP Management configuration options.

Limiting SNMP Access through IP Addresses

An additional level of security is provided by:

- Limiting the IP addresses of NMSs that can access the DSU/CSU.
- Performing validation checks on the IP address of SNMP management systems attempting to access the DSU/CSU.
- Specifying the access allowed for the authorized NMS when IP address validation is performed.

The SNMP NMS Security Options screen provides the configuration options that determine whether security checking is performed on the IP address of SNMP management systems attempting to communicate with the unit.

Make sure that SNMP Management is set to Enable.

Menu selection sequence:
Main Menu → *Configuration* → *Management and Communication* → *General SNMP Management* → *SNMP Management: Enable*

See *Configuring General SNMP Management* in Chapter 3, *Configuration,* for more information about SNMP management configuration options.

▶ Procedure

To limit SNMP access through IP addresses:

1. Select the SNMP NMS Security options:

   Main Menu → *Configuration* → *Management and Communication* → *SNMP NMS Security*

2. Select and set the following configuration options, as appropriate.

To . . .	Set the configuration option . . .
Enable IP address checking	NMS IP Validation to Enable.
Specify the number (between 1 and 10) of SNMP management systems that are authorized to send SNMP messages to the DSU/CSU	Number of Managers to the desired number.
Specify the IP address(es) that identifies the SNMP manager(s) authorized to send SNMP messages to the unit	NMS *n* IP Address to the appropriate IP address.
Specify the access allowed for an authorized NMS when IP address validates is performed	Access Level to Read or Read/Write.

3. Save your changes.

See *Configuring SNMP NMS Security* in Chapter 3, *Configuration,* for more information about SNMP NMS Security configuration options.

Creating a Login

A login is required if security is enabled. (Security is enabled by the configuration options Login Required for the communication port, modem port, and Telnet Login Required or FTP Login Required for a Telnet or FTP Session.) Up to six login ID/password combinations can be created using ASCII text, and each login must have a specified access level. Logins must be unique and they are case-sensitive.

▶ Procedure

To create a login record:

1. Select Administer Logins.

   Main Menu → Control → Administer Logins

2. Select New, and set the following configuration options, as appropriate.

In the field . . .	Enter the . . .
Login ID	ID of 1 to 10 characters.
Password	Password from 1 to 10 characters.
Re-enter password	Password again to verify that you entered the correct password into the device.
Access Level	Access level: 1, 2, or 3. ■ Level-1 – User can add, change, and display configuration options, save, and perform device testing. ■ Level-2 – User can monitor and perform diagnostics, display status and configuration option information. ■ Level-3 – User can only monitor and display status and configuration screens. **CAUTION:** Make sure at least one login is set up for Level-1 access or you may be inadvertently locked out.

NOTE:

Should you be locked out inadvertently, see *Resetting the Unit and Restoring Communication* in Chapter 6, *Troubleshooting*.

3. Save your changes.

   When Save is complete, the cursor is repositioned at the Login ID field, ready for another entry.

See *Configuring SNMP NMS Security* in Chapter 3, *Configuration,* for more information about security configuration options.

Modifying a Login

Logins are modified by deleting the incorrect login and creating a new one.

Deleting a Login

▶ Procedure

To delete a login record:

1. Select Administer Logins.

   Main Menu → Control → Administer Logins

2. Page through login pages/records using the PgUp or PgDn function keys until the login to be deleted is displayed.
3. Select Delete.
4. Save your deletion.

   When the deletion is complete, the number of login pages/records reflects one less record, and the record before the deleted record reappears.

   Example:
   Page 2 of 4 is changed to Page 2 of 3.

Operation and Maintenance

5

This chapter includes the following:

- *Displaying System Information* on page 5-2
- *Viewing LEDs and Control Leads* on page 5-3
  - *LED Descriptions*
- *Device Messages* on page 5-6
- *Status Information* on page 5-10
  - *System and Test Status Messages*, which includes:
    - *Self-Test Results Messages*
    - *Last System Reset Date and Time*
    - *Health and Status Messages*
    - *Test Status Messages*
  - *Time Slot Assignment Status*
- *IP Routing Table* on page 5-15
- *Performance Statistics* on page 5-17
  - *Clearing Performance Statistics*
  - *ESF Line Performance Statistics*
  - *Ethernet Performance Statistics*
- *FTP File Transfers* on page 5-23
- *FTP File Transfers* on page 5-23
  - *Upgrading System Software*
  - *Determining Whether a Download Is Complete*
  - *Changing Software*

Displaying System Information

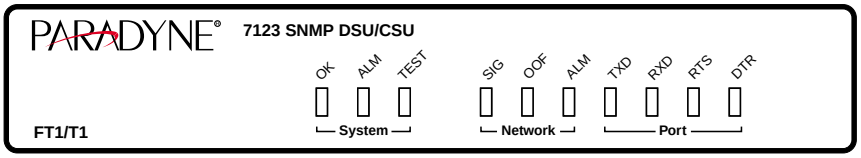
Use the Identity screen to view identification information about the 7123 SNMP DSU/CSU. This information is useful if you are purchasing additional or replacement units and/or making firmware upgrades.

Main Menu→Status→Identity

View this field . . .	**To find the . . .**
System Name	Domain name for this SNMP-managed node (up to 255 ASCII characters).
System Contact	Contact person for this SNMP-managed node.
System Location	Physical location for this SNMP-managed node.
NAM	
NAM Type	Type of unit installed, referred to as a network access module, or NAM. This card type is supported by the SNMP SysDescr Object.
Hardware Revision	Unit's hardware version. Format *nnnn-nnx* consists of a 4-digit number, followed by two digits and one alphabetic character.
Current Software Revision	Software version currently being used by the unit. Format *nn.nn.nn* consists of a 6-digit number that represents the major and minor revision levels.
Alternate Software Revision	Software version that has been downloaded into the unit, but has not yet been implemented. Format is the same as for the Current Software Revision. ■ **`In Progress`** indicates that the flash memory is currently being downloaded. ■ **`Invalid`** indicates that no download has occurred or the download was not successful
Serial Number	Unit's 7-character serial number.
Ethernet MAC Address	Media Access Control (MAC) address assigned to the Ethernet port during manufacturing.

Viewing LEDs and Control Leads

The 7123 SNMP DSU/CSU's faceplate includes LEDs (light-emitting diodes) that provide status on the unit and its interfaces.



01-17031

The Display LEDs and Control Leads screen allows you to monitor a remote unit and is useful when troubleshooting control lead problems. The appropriate interfaces are shown on this screen, with the appropriate status highlighted.

Main Menu → Status → Display LEDs and Control Leads

Display LEDs & Control Leads Screen

```
main/status/leds                                                    7123
Device Name: Node A                                  09/09/2001 05:01

                        DISPLAY LEDS & CONTROL LEADS

                                T1 DSU/CSU

        GENERAL         NETWORK1            PORT-1
        OK              Sig                 OK
        Alarm           OOF                 TXD
        Test            Alm                 RXD
                                            DTR
                                            RTS

--------------------------------------------------------------------------------
                    ESC for previous menu          MainMenu       Exit
 Refresh
```

LEDs and control leads in an ON state are shown in inverse video.

Refresh the screen to view control lead transitions. LED and control lead descriptions are in the sections that follow.

LED Descriptions

Table 5-1, General Status LEDs, identifies the alarms that cause the Alarm LED to light. See Table 5-2, Network Interface LEDs, and Table 5-3, User Data Port LED, for network and user data port interface LED information.

Table 5-1. General Status LEDs

Label	Indication	Color	What It Means
OK	Power and Operational Status	Green	ON – DSU/CSU has power and it is operational. OFF – DSU/CSU is in a power-on self-test, or there is a failure.
ALM	Operational Alarm (Fail)	Red	ON – DSU/CSU has just been reset, or an error or fault has been detected. Error/fault/alarm conditions: ■ Alarm Indication Signal (AIS) ■ CTS Down ■ DTR Down ■ Exceeded Error Rate (EER) ■ Loss of Signal (LOS) ■ Out of Frame (OOF) ■ Primary Clock Failed ■ Self-Test Failed ■ Two Level-1 Users Accessing Device ■ Yellow Alarm Signal OFF – No failures have been detected. These alarms appear on the System and Test Status screen. See *Health and Status Messages* on page 5-12 for additional information.
TST	Test Mode	Yellow	ON – Loopback or test pattern is in progress, initiated locally, remotely, or from the network. OFF – No tests are active.

Table 5-2. Network Interface LEDs

Label	Indication	Color	What It Means
SIG	Signal	Green	ON – A recoverable signal is present on the network interface. OFF – The signal cannot be recovered from the network interface. An LOS condition exists.
OOF	Out of Frame	Yellow	ON – At least one OOF was detected during the sampling period. OFF – No OOFs were detected during the sampling period.
ALM	Alarm	Yellow	ON – An alarm condition is present on the network interface. Current alarm conditions: ■ Alarm Indication Signal (AIS) ■ Excessive Error Rate (EER) ■ Loss of Signal (LOS) ■ Loss of Frame (LOF) ■ Out of Frame (OOF) ■ Yellow Alarm Signal OFF – No alarm condition is present on the network interface.

Table 5-3. User Data Port LED

Label	Indication	Color	What It Means
TXD	Transmitted Data	Green	ON – Receiving a 0 from the DTE. OFF – Receiving a 1 from the DTE.
RXD	Received Data	Green	ON – Sending a 0 to the DTE. OFF – Sending a 1 to the DTE.
RTS	Request to Send	Green	ON – DTE is activating a control signal to indicate readiness to transmit data.
DTR	Data Terminal Ready	Green	ON – DTE is activating a control signal to indicate readiness for operation.
OK	Operational Status	(No LED)	ON – The interchange circuits for the port are in the correct state to send and receive data. OFF – The port is idle.

Device Messages

These messages appear in the messages area at the bottom of the screens. All device messages are listed in alphabetical order.

Table 5-4. Device Messages (1 of 4)

Message	What It Indicates	What To Do
Access level is *n*, Read-only.	User's access level is 2 or 3; user is not authorized to change configurations.	No action is needed.
Already Active	Test selected is already running.	■ Allow test to continue. ■ Select another test. ■ Stop the test.
Blank Entries Removed	New had been selected from the Administer Logins screen, no entry was made, then Save was selected.	■ No action is needed. ■ Reenter the Login ID, Password, and Access Level.
Cannot Save – no Level 1 Login IDs	Security was being set up, but all the logins were assigned either Level-2 or Level-3 access.	Notify your service provider.
Command Complete	Configuration has been saved or all tests have been aborted.	No action is needed.
Connection Refused *(Seen at an FTP terminal.)*	Two menu-driven user interface sessions are already in use when a Telnet session was attempted.	Wait and try again.
File Transfer Complete *(Seen at an FTP terminal.)*	A file transfer was performed successfully.	Switch to the newly downloaded software. See *Changing Software* on page 5-26.
File Transfer Failed – Invalid file *(Seen at an FTP terminal.)*	A file transfer was attempted, but it was not successful.	■ Try again, making sure you type the filename correctly. ■ Exit the FTP session, or download another file. See *Changing Software* on page 5-26.
Invalid Character (*x*)	A non-valid printable ASCII character has been entered.	Reenter information using valid characters.
Invalid date: must be mm/dd/yyyy	A non-valid date was entered on the System Information screen.	Reenter the date in the month/day/4-digit year format.

Table 5-4. Device Messages (2 of 4)

Message	What It Indicates	What To Do
Invalid date and/or time	A non-valid date or time was entered on the System Information screen. The date does not exist (e.g., February 30th).	Reenter the date in the month/day/4-digit year format and/or time in the hour:minutes:seconds format.
Invalid time: must be hh:mm:ss	A non-valid system time was entered on the System Information screen.	Reenter the time in the hour:minutes:seconds format.
Invalid – Already Active	A test was already in progress when it was selected.	No action is needed.
Invalid Password	Login is required and an incorrect password was entered; access is denied.	■ Try again. ■ Contact your system administrator to verify your password.
Invalid Test Combination	A conflicting loopback or pattern test was in progress when Start was selected to start another test, or was active on the same or another interface when Start was selected.	■ Wait until other test ends and message clears. ■ Cancel all tests from the Test screen (Path: main/test). ■ Stop the test from the same screen the test was started from.
Limit of six Login IDs reached	An attempt to enter a new login ID was made, and the limit of six login/password combinations has been reached.	■ Delete another login/password combination. ■ Reenter the new login ID.
No Security Records to Delete	Delete was selected from the Administer Login screen, and no security records had been defined.	■ No action is needed. ■ Enter a security record.
Password Matching Error – Re-enter Password	Password entered in the Re-enter Password field of the Administer Logins screen does not match what was entered in the Password field.	■ Try again. ■ Contact your system administrator to verify your password.

Table 5-4. Device Messages (3 of 4)

Message	What It Indicates	What To Do
Permission Denied *(Seen at an FTP terminal.)*	A file transfer was attempted, but the: ■ User did not have Level 1 security. ■ Wrong file was specified when the **put** command was entered. ■ User attempted to upload a program file from the unit.	■ See your system administrator to get your security level changed. ■ Try again, entering the correct file with the **put** command. ■ Enter the **put** command instead of a **get** command; you can only transfer files to the unit, not from it. See *Upgrading System Software* on page 5-25.
Please Wait	Command takes longer than 5 seconds.	Wait until message clears.
Port Inactive	The port is disabled, or it supports synchronous data and is configured for leased line mode when a DTE Loopback was started.	No action is needed.
Resetting Device, Please Wait ...	Yes (or y) was entered in the **`Reset COM Port usage`** field of the System Paused menu.	No action is needed.
Save Cancelled	Configuration options were changed, but the Esc key was pressed or No was entered in response to the **`Save Changes?`** prompt.	No action is needed.
Test Active	No higher priority health and status messages exist, and a test is running.	■ Contact service provider if test initiated by the network. ■ Wait until the test ends and message clears. ■ Cancel all tests from the Test screen (Path: main/test). ■ Stop the test from the same screen the test was started from.

Table 5-4. Device Messages (4 of 4)

Message	What It Indicates	What To Do
User Interface Already in Use	Two Telnet sessions are already in use when an attempt to access the menu-driven user interface through the COM port is made. IP addresses and logins of the users currently accessing the interface are also provided.	■ Wait and try again. ■ Contact one of the IP address user and request that they log off.
User Interface Idle	Previously active session is now closed/ended, and access via the COM port is now available.	Log on to the DSU/CSU.
	Session has been ended due to timeout.	No action is needed.

Status Information

Status information is useful when monitoring the DSU/CSU. The following illustration shows the Status menu for the 7123 DSU/CSU.

Status Menu

```
main/status                                                          7123
Device Name: Node A                                    09/09/2001 05:02

                                   STATUS

                            System and Test Status
                            Time Slot Assignment Status
                            IP Routing Table (Management Traffic)
                            Performance Statistics
                            Display LEDs and Control Leads
                            Identity









--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
```

NOTE:

Status messages in the following sections are in alphabetical order.

System and Test Status Messages

System and test status information is selected from the Status menu.

Main Menu → Status → System and Test Status

The following information is included on this screen:

- *Self-Test Results Messages*
- *Last System Reset Date and Time*
- *Health and Status Messages*
- *Test Status Messages*

Self-Test Results Messages

One of these self-test result messages appears in the Self-Test Results field at the top of the System and Test Status screen.

Table 5-5. Self-Test Results Messages

Message	What It Indicates	What To Do
Failure *xxxxxxxx*	An internal failure occurred *(xxxxxxxx* represents an 8-digit hexadecimal failure code used by service personnel). Record the failure code before resetting the unit; otherwise, the error information will be lost.	1. Record the failure code. 2. Reset the unit. 3. Contact your service representative.
Passed	No problems were found during power-on or reset.	No action needed.

Last System Reset Date and Time

This field indicates the last time the DSU/CSU was reset. It appears after the Self-Test Results field at the top of the System and Test Status screen.

- Date is in mm/dd/yyyy format (month/day/year).
- Time is in mm:ss format (minutes:seconds).

Health and Status Messages

The following table provides Health and Status messages that apply to the 7123 DSU/CSU.

Table 5-6. Health and Status Messages (1 of 2)

Message	What It Indicates
AIS at Network 1	An Alarm Indication Signal (AIS) is received by the network interface. AIS is an unframed, all ones signal. Possible reasons include: ■ Upstream DSU/CSU is transmitting AIS (keep-alive signal). ■ The network is transmitting an AIS.
CTS down to Port-1 Device	The user data port CTS control lead on the DSU/CSU is off.
DTR Down from Port-1 Device	The DTR control lead from the device connected to the user data port is deasserted.
EER at Network 1	The error rate of the received network signal exceeds the currently configured threshold. This condition only occurs if the network interface is configured for ESF framing. This condition clears when the error rate falls below the threshold value, which may take up to 15 minutes.
Ethernet Link Down	The Ethernet port is enabled, but communication between the management system and the unit is not currently possible on the port.
LOS at Network 1	A Loss of Signal (LOS) condition is detected on the network interface. Clears when the ratio of ones to zeros received is greater than or equal to 12.5%. Possible reasons include: ■ Network cable problem. ■ No signal is being transmitted at the far-end DSU/CSU. ■ T1 facility problem.
Network Com Link Down	The communication link for the COM port is down, and the COM port is configured for Net Link.
OOF at Network 1	An Out of Frame (OOF) condition is detected on the network interface. Possible reasons include: ■ Incompatible framing format between the network and the DSU/CSU. ■ Network cabling problem. ■ T1 facility problem.

Table 5-6. Health and Status Messages (2 of 2)

Message	What It Indicates
Primary Clock Failed	A failure of the primary clock source configured for the unit is detected and the unit's internal clock is providing the timing. This condition clears when the configured primary clock is restored.
Two Level-1 Users Accessing Device	Two Level 1 users are already using the menu-driven user interface; only two sessions can be active at one time.
Yellow at Network 1	A yellow alarm signal is received on the network interface. Possible reasons include: ■ Network cable problem. ■ T1 facility problem.

Test Status Messages

These test messages appear in the right column of the System and Test Status screen. You have the option of allowing the test to continue or aborting the test. See Chapter 6, *Troubleshooting*, for more information on tests, including how to start and stop them.

Table 5-7. Test Status Messages

Message	What It Indicates
DCLB Active, Port-1	A Data Channel V.54 Loopback (DCLB) is active on the data for the user data port.
DTE External LB Active, Port-1	An external DTE Loopback is running on the user data port.
DTE Init. Ext LB Active, Port-1	The DTE has initiated an external DTE Loopback on the user data port.
DTPLB Active, Port-1	A Data Terminal Payload Loopback (DTPLB) is active for the specified slot and port.
Lamp Test Active	The Lamp Test is active, causing the LEDs on the faceplate to flash on and off.
LLB Active, Network 1	A network Line Loopback (LLB) is active on the specified interface.
Monitor *Pttn* Active, *[Interface]*	A Monitor Pattern test is active on the specified interface.
No Test Active	No tests are currently running.
PLB Active, Network 1	A Payload Loopback (PLB) is active on the specified interface.
Send *Pttn* Active, *[Interface]*	A Send Pattern test is active on the specified interface.

Time Slot Assignment Status

Time Slot assignments are made using the Time Slot Assignment configuration option. See *Assigning Time Slots/Cross Connections* in Chapter 3, *Configuration*, for making time slot assignments. Use the Timeslot Assignment Status screen to display time slot assignments for the network channels.

Displaying Network Time Slot Assignments

Use the Network Timeslot Assignment Status screen to display DS0 assignments for each DS0 on the network interface.

Main Menu→ Status→ Timeslot Assignment Status →Network

The Network Timeslot Assignment Status screen displays 24 two-field entries in three rows. Together, each two-field entry defines the assignment for one network interface time slot. The top field represents the time slot of the network interface. The bottom field represents the cross-connect status of the associated (top field) network time slot.

Network Timeslot Assignment Status Screen Example

```
main/status/timeslot/net_display                                        7123
Device Name: Node A                                        09/09/2001 05:03


                    NETWORK 1 TIMESLOT ASSIGNMENT STATUS

  N01      N02      N03      N04      N05      N06      N07      N08
Unassign Unassign Unassign Unassign Unassign Unassign Unassign Unassign

  N09      N10      N11      N12      N13      N14      N15      N16
Unassign Unassign Unassign Unassign Unassign Unassign Unassign Unassign

  N17      N18      N19      N20      N21      N22      N23      N24
Unassign Unassign Unassign Unassign Unassign Unassign Unassign Unassign









--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
 Refresh
```

The following information is available for network interface time slots (N01– N24):

The Cross Connect Status Field (bottom) . . .	Indicates . . .
Unassgn	The time slot is unassigned.
Port-1	The synchronous data port (Port-1) is assigned to the network interface time slot (01 to 24).

IP Routing Table

Use the IP Routing Table to see all the routes configured in the DSU/CSU.

Main Menu→Status→IP Routing Table

IP Routing Table Screen Example

```
main/status/ip_rout                                                    7123
Device Name: Node A                                        09/09/2001 05:04

                                                                Page 1 of 2

                                IP ROUTING TABLE

  Destination       Mask            Gateway       Hop   Type   Interface     TTL
135.001.220.000  255.255.255.000  135.042.001.254  1    Loc    Ethernet      999
135.001.221.000  255.255.255.000  135.042.001.254  1    Loc    COM            99
135.001.220.000  255.255.255.000  135.042.001.254  1    Loc    COM           999
135.001.222.111  255.255.255.000  135.026.001.254  1    RIP    Ethernet       30

--------------------------------------------------------------------------------
                                ESC for previous menu      MainMenu   Exit
 Refresh     PgDn   PgUp
```

The table is sorted by the Destination IP address, from the lowest number to the highest. If no routes exist, the **No Routes** message appears instead of routing information.

Table 5-8. IP Routing Table Values (1 of 2)

Column	What It Indicates
Destination	The Destination IP Address for the route: ■ 001.000.000.000 – 223.255.255.255
Mask	The Destination Subnet Mask for the route: ■ 000.000.000.000 – 225.255.255.255 for network routes ■ FFF.FFF.FFF.FFF for host routes ■ 127 may appear as well. It is a reserved number.
Gateway	The Gateway IP Address for the route: ■ 001.000.000.000 – 223.255.255.255
Hop	The number of hops in the route to the destination (1–15). If 16 appears, the route is in the process of being aged out.

Table 5-8. IP Routing Table Values (2 of 2)

Column	What It Indicates
Type	The method used to add the route to the table. ■ RIP: The route was discovered through Routing Information Protocol. The route remains until its TTL (Time to Live) expires, a better route is provided via RIP, or there is a power reset. ■ Loc: The route was added due to the DSU/CSU's local configuration; a Default IP Address or an SNMP Manager Initial Route Destination have been configured. The route remains until the unit's configuration changes. ■ NMS: The route was added by a Network Management System using SNMP (Simple Network Management Protocol). The route remains until there is a power reset of the unit. ■ ICMP: The route was added because an ICMP (Internet Control Management Protocol) redirect message was received from a router indicating a better route to the destination. That is, a datagram was sent to a router and the router is informing the datagram source through an ICMP redirect message of a better route. ■ Tmp: The route was added as a temporary route in order to respond to an IP packet that was received. The route remains until its TTL expires or there is a power reset.
Interface	Specifies the interface to be used to reach the destination. ■ COM: Communications port ■ Ethernet: Ethernet port ■ Internal: The interface to be used for software loopbacks or internal device functions in order to reach the destination.
TTL	The Time to Live that was set for the route, in seconds: 1–999

Performance Statistics

Use the Performance Statistics menu to display statistical information for a selected interface. Statistical information is useful when trying to determine the severity and frequency or duration of a condition.

Main Menu → Status → Performance Statistics

Physical and link layer statistics (Layers 1 and 2) are collected on the port. The following menu shows the performance statistics that can be selected.

Performance Statistics Menu

```
main/status/performance                                                    7123
Device Name: Node A                                          09/09/2001 05:05

                            PERFORMANCE STATISTICS

                            ESF Line
                            Ethernet
                            Clear All Statistics









--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
```

Clearing Performance Statistics

Performance statistics counters can be reset to the baseline when using a directly-connected asynchronous terminal and your security Access Level is Level-1. This feature is useful when troubleshooting problems.

Statistic counters are not actually cleared using this feature. True statistic counts are always maintained, and they can be viewed from an SNMP NMS. However, since statistics can be cleared locally, the statistics viewed via the menu-driven user interface may be different from those viewed from the NMS.

▶ Procedure

To clear all statistics:

Performance Statistics → Clear All Statistics

▶ Procedure

To clear specific statistics:

- Use the ClrNearStats or ClrFarStats function key to reset all near-end or all far-end Extended SuperFrame (ESF) line performance statistics.

  Performance Statistics → ESF Line

ESF Line Performance Statistics

These statistics appear when ESF Line is selected from the Performance Statistics menu for the network interface.

Main Menu→Status→Performance Statistics→ESF Line

Only seven T1 network statistical intervals appear on the screen at any one time. You can choose which intervals to display on your screen by entering:

- Interval Number (01–96)

  – or –

- Time (Hours and Minutes)

NOTES:

— Interval 01 is the interval that occurred just prior to the current one; Interval 02 is two intervals prior to the current one, and so on.

— Selecting a specific time is useful when the approximate time at which a specific event occurred is known.

Edit any of the interval or time fields on lines 10, 13, or 16. When Enter is pressed, the values change to the selected range.

To select intervals . . .	**You must enter an interval or time on . . .**
Occurring on and before a selected interval or time	Line 10. The display will include the selected interval plus the 6 intervals recorded before it.
Bracketing a selected interval or time	Line 13. The display will include the selected interval plus the 3 intervals recorded before it and the 3 intervals recorded after it.
Occurring on and after a selected interval or time	Line 16. The display will include the selected interval plus the 6 intervals recorded after it.

ESF Line Performance Statistics Screen Example

```
main/status/performance/esf                                          7123
Device Name: Node A                                   09/09/2001 05:06
                  Network 1 ESF LINE PERFORMANCE STATISTICS
Current Interval Timer                                 ESF Error Events
Near=123    Far = 124                                Near = 15   Far = 12

                 ---ES--   --UAS--   --SES--   --BES--   --CSS--   -LOFC--
          Time   Near Far  Near Far  Near Far  Near Far  Near Far  Near Far
 Current: 10:37    0   0     0   0     0   0     0   0     0   0     0   0
Line 10 ─ Int 01: 10:35    0   0     0   0     0   0     0   0     0   0     0   0
  Int 02: 10:20    0   0     0   0     0   0     0   0     0   0     0   0
  Int 03: 10:05    0   0     0   0     0   0     0   0     0   0     0   0
Line 13 ─ Int 04: 09:50    0   0     0   0     0   0     0   0     0   0     0   0
  Int 05: 09:35    0   0     0   0     0   0     0   0     0   0     0   0
  Int 06: 09:20    0   0     0   0     0   0     0   0     0   0     0   0
Line 16 ─ Int 07: 09:05    0   0     0   0     0   0     0   0     0   0     0   0

  Worst Interval:  24  24    14  14    14  14    09  09    18  16    44  44
Near Tot(valid 96):  00010     00000     00000     00000       002       003
Far  Tot(valid 96):  00010     00000     00000     00000       002       003
-------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu    Exit
 Refresh     PgDn   PgUp     ClrFarStats   ClrNearStats
Select: 01, 02, 03, 04, 05, 06, 07, 08, 09 ...
```

For the ESF line performance statistics, the following performance statistics are kept for each 15-minute interval over the past 24-hour period. A Near set and a Far set are kept for each statistic. The Far set is based on information kept by the unit at the other end of the local loop and is only available when ANSI performance report messages are enabled in the unit.

Summary information that appears near the top of the screen includes:

- **Near/Far Current Interval Timer** – Contains the number of seconds that have elapsed in the current 15-minute interval for the near or far information, which can show a value up to 900 seconds.
- **Near/Far ESF Error Events** – Maintains a count of ESF error events, as specified by AT&T TR 54016, which counts CRC and OOF events. A maximum of 65,535 error events can be counted. Once 65535 is reached, it stays at that number until the network issues a reset command.

The following performance statistics are collected for ESF line conditions.

Statistic	What It Indicates
Errored Seconds (ES)	Any second with one or more ESF Error events.
Unavailable Seconds (UAS)	Any second in which service is unavailable. Begins incrementing at the onset of 10 consecutive seconds of severely errored seconds (SES), and stops incrementing after 10 consecutive seconds of no SESs.
Severely Errored Seconds (SES)	Any second with 320 or more CRC errors or one or more Out Of Frame (OOF) events.
Bursty Errored Seconds (BES)	Any second with more than one, but less than 320 CRC errors.
Controlled Slip Seconds (CSS)	Any second with one or more controlled slips (a replication or deletion of a DS1 frame by the receiving device). This is collected for network performance statistics only.
Loss of Frame Count (LOFC)	The number of Loss of Frame conditions.
Worst Interval	The largest number of seconds for either ES, UAS, SES, BES, or CSS, or the greatest Loss of Frame Count (LOFC). If more than one interval contains the same worst value, then the oldest interval is displayed.

Ethernet Performance Statistics

The following statistics appear when Ethernet is selected from the Performance Statistics menu.

Main Menu → Status → Performance Statistics → Ethernet

Statistic	What It Indicates
Port Rate (Mbps)	The operating rate as detected on the Ethernet port. One of the following may appear for this statistic: ■ Disconnected – The line is not connected. ■ 10 Mbps or 100 Mbps – The Ethernet port is operating at this rate. ■ Disabled – The Ethernet port has been disabled.
Duplex	The duplex mode detected on the Ethernet port. One of the following may appear for this statistic: ■ Disconnected – The line is not connected. ■ Full – The Ethernet port is operating in full duplex mode (4-wire). ■ Half – The Ethernet port is operating in half duplex mode (2-wire). ■ Disabled – The Ethernet port has been disabled.
Frames Transmitted	The number of successfully transmitted frames on the port.
Frames Received	The number of frames received on the port.
Errored Frames	The number of errors detected on the port. Possible errors include: ■ Internal transmit and receive errors ■ Transmitter and receiver overruns ■ Receive checksum errors ■ Alignment errors ■ Long frames
Excessive Collisions	The number of failed frame transmissions due to excessive collisions.
Carrier Sense Errors	The number of times the carrier sense condition was lost, or was never asserted, during frame transmissions.
Deferred Transmissions	The number of delayed first transmissions due to the line being busy.

FTP File Transfers

The 7123 DSU/CSU supports a standard File Transfer Protocol (FTP) server over Transmission Control Protocol (TCP). A complete binary image of the configuration files can be copied to a host to provide a backup. To use this feature, the unit must be configured to support Telnet and FTP Sessions.

Using this feature, you can transfer configuration files to and from a 7123 DSU/CSU and program files to a 7123 DSU/CSU through the COM port or Ethernet port.

Be aware of the following rules when doing a file transfer:

- You must have Access Level 1 permission to use the **put** and **get** commands.
- You cannot **put** a configuration file to the factory.cfg or current.cfg files under the system directory. Configuration files should be put to a customer file (cust1.cfg or cust2.cfg), then loaded into the downloaded unit's Current Configuration via the menu-driven user interface.
- You can only **put** a NAM program file (nam.ocd) into a DSU/CSU. You cannot **get** a program file from the DSU/CSU to a host.
- Before putting a download file, you must use the **bin** binary command to place the data connection in binary transfer mode.

You initiate an FTP session to a 7123 DSU/CSU in the same way as you would initiate an FTP to any other IP-addressable device.

▶ Procedure

To initiate an FTP session:

1. Start the FTP client program on your host. For example, on a UNIX host, type **ftp**, followed by the DSU/CSU's IP address.
2. If a login and password are required (see *Creating a Login* in Chapter 4, *Security and Logins*), you are prompted to enter them. If not, press Enter.

   The FTP prompt appears.

   The starting directory is the root directory (/). Use standard FTP commands during the FTP session, as well as the following remote FTP commands.

Command	Definition
cd *directory*	Change the current directory on the DSU/CSU to the specified *directory*.
dir [*directory*]	Print a listing of the directory contents in the specified *directory*. If no directory is specified, the current one is used.
get *file1* [*file2*]	Copy a file from the remote directory of the DSU/CSU to the local directory on the host (for configuration files only).
remotehelp [*command*]	Print the meaning of the command. If no argument is given, a list of all known commands is printed.
ls [*directory*]	Print an abbreviated list of the specified directory's contents. If no directory is specified, the current one is used.
put *file1* [*file2*]	Copy *file1* from a local directory on the host to *file 2* in the current directory of the DSU/CSU. If *file2* is not specified, the file will be named *file1* on the DSU/CSU.
recv *file1* [*file 2*]	Same as a **get**.
send *file1* [*file 2*]	Same as a **put**.
pwd	Print the name of the current directory of the DSU/CSU.
bin	Places the FTP session in binary-transfer mode.

Upgrading System Software

If you need to upgrade the DSU/CSU's program code, you must transfer the upgrade of the **nam.ocd** file in the system memory directory using the **put** command.

NOTE:

Upgrades can be performed through the COM port if Port Use is set to Net Link (see Table 3-10, Communication Port Options, in Chapter 3, *Configuration*).

▶ Procedure

To download software:

1. Initiate an FTP session to the device that you are upgrading.
2. Type **bin** to enter binary transfer mode.
3. Type **hash** to enter hash mode if you want to monitor the progress of the upgrade, provided this function is supported by your equipment.
4. Type **cd system** to change to the system directory.
5. Perform a **put** of R*xxxxxx*.ocd (*xxxxxx* being the software release number) to the nam.ocd file to start the upgrade.

   During the download, a series of hash marks (#) appear. When the hash marks stop appearing, there is a pause of about 30 seconds before the **`nam.ocd: File Transfer Complete`** message appears. Do not exit from FTP during the pause.

If the message displayed is . . .	Then . . .
nam.ocd: File Transfer Complete	The download was successful. The file is loaded into system memory.
nam.ocd: File Transfer Failed – Invalid file	The file is not valid for this DSU/CSU. A different R*xxxxxx*.ocd file will need to be downloaded. Repeat the step or end the FTP session.

Determining Whether a Download Is Complete

To see whether a download has completed, check the Identity screen.

Main Menu → Status → Identity

Check Alternate Software Rev. under the NAM Identity column.

- If a software revision number appears, the file transfer is complete.
- If **`In Progress`** appears, the file is still being transferred.
- If **`Invalid`** appears, no download has occurred or the download was not successful.

Changing Software

Once a software upgrade is downloaded, it needs to be activated. When activated, the unit resets, then executes the downloaded software. With this feature, you control when the upgrade software is implemented.

▶ Procedure

To switch to the new software:

1. Go to the Control menu, and select Select Software Release.

   Main Menu → Control → Select Software Release

   The currently loaded software version and the new release that was just transferred are shown.

   If the download failed, **`Invalid`** appears in the Alternate Release field instead of the new release number. Repeat the procedure in *Upgrading System Software* on page 5-25 if this occurs.

2. Select Switch&Reset.

3. Enter Yes to the **`Are you sure?`** prompt. The unit resets and begins installing the newly transferred software.

4. Verify that the new software release was successfully installed as the Current Software Revision.

   Main Menu → Status → Identity

   NOTE:

   If someone opens a Telnet session and accesses the unit's Identity screen while the unit is downloading software, the **`In Progress...`** message appears in the Alternate Software Revision field.

   See *Displaying System Information* on page 5-2 to see what is included on the unit's Identity screen.

Troubleshooting

6

This chapter includes the following:

- *Problem Indicators* on page 6-2
- *Resetting the Unit and Restoring Communication* on page 6-3
  - *Resetting the Unit from the Control Menu*
  - *Resetting the Unit By Cycling the Power*
  - *Restoring Communication with an Improperly Configured Unit*
- *Alarms* on page 6-5
- *Troubleshooting Device Problems* on page 6-8
- *Tests Available* on page 6-9
  - *Test Timeout Feature*
- *Starting and Stopping a Test* on page 6-10
  - *Aborting All Tests*
- *Physical Tests* on page 6-12
  - *Line Loopback*
  - *Payload Loopback*
  - *Send Line Loopback*
  - *Send and Monitor Pattern Tests*
  - *DTE Loopback*
- *IP Ping Test* on page 6-18
- *Lamp Test* on page 6-19

Problem Indicators

The 7123 SNMP DSU/CSU provides a number of indicators to alert you to possible problems:

Indicators . . .	**See . . .**
LEDs	*Viewing LEDs and Control Leads* in Chapter 5, *Operation and Maintenance*. *Main Menu → Status → Display LEDs and Control LEDs*
Health and status	*Health and Status Messages* in Chapter 5, *Operation and Maintenance*. *Main Menu → Status → System and Test Status* Messages also appear at the bottom of any menu-driven user interface screen.
Performance statistics	*Performance Statistics* in Chapter 5, *Operation and Maintenance*, to help you determine how long a problem has existed.
Alarm conditions that will generate an SNMP trap	*Alarms* on page 6-5.
SNMP traps	Appendix B, *SNMP MIBs and Traps*. Traps supported include warm-start, authentication-failure, enterprise-specific (those specific to the unit), link-up, and link-down.

Resetting the Unit and Restoring Communication

You can reset the unit in one of four ways:

- Reset it from the Control menu.
- Cycle the power.
- Reset the configuration options for the COM port, or reload the factory default settings.
- Set the appropriate MIB object from NMS (see your NMS documentation).

The unit performs a self-test when it is reset.

Resetting the Unit from the Control Menu

Use this procedure to initiate a reset and power-on self-test of the unit.

▶ Procedure

To reset the unit from the Control menu:

1. From the Main Menu screen, select Control.
2. Select Reset Device and press Enter. The **`Are You Sure?`** prompt appears.
3. Type **y** (Yes) and press Enter. The unit reinitializes itself, performing a self-test.

Resetting the Unit By Cycling the Power

Disconnecting, then reconnecting the power cord resets the unit.

Restoring Communication with an Improperly Configured Unit

Improperly configuring the unit could render the menu-driven user interface inaccessible. If this occurs, connectivity to the unit can be restored via a directly connected asynchronous terminal.

▶ Procedure

To reset COM port settings:

1. Configure the asynchronous terminal to operate at 19.2 Kbps, using a character length of 8 bits, with one stop bit, and no parity. In addition, set Flow Control to None.
2. Reset the unit, then hold the Enter key down until the System Paused screen appears. (See *Resetting the Unit and Restoring Communication* on page 6-3 for other methods of resetting the unit.)
3. Tab to the desired prompt, and type **y** (Yes) at one of the prompts.

If selecting . . .	The following occurs . . .
Reset COM Port usage	■ Port Use is set to Terminal so the asynchronous terminal can be used. ■ Data Rate (Kbps), Character Length, Stop Bits, and Parity are reset to the factory defaults. ■ Unit resets itself.
Reload Factory Defaults	■ All configuration and control settings are reset to the Default Factory Configuration, overwriting the current configuration. ■ Unit resets itself. **CAUTION:** This causes the current configuration to be destroyed and a self-test to be performed.

If no selection is made within 30 seconds, or if No (**n**) is entered, the unit resets itself and no configuration changes are made.

Once the unit resets itself, connectivity is restored and the Main Menu screen appears.

Alarms

Table 6-1, Alarm Conditions, describes the alarm conditions that will generate an SNMP trap for a physical interface. These alarm conditions also generate Health and Status messages seen on the System and Test Status screen.

Main Menu → Status → System and Test Status

Table 6-1. Alarm Conditions (1 of 3)

Alarm Condition	What It Indicates	What To Do
AIS at Network 1	An Alarm Indication Signal (AIS) is being received by the interface. AIS is an unframed, all ones signal.	For the network interface, report the problem to your T1 service provider.
CTS down to Port-1 Device	The CTS control lead on the device's interface is off.	Check DTR and RTS from Port-1. ■ Verify that the port is enabled. ■ Check DTR from the user data port.
DTR Down from Port-1 Device	The DTR control lead on the device connected to the specified port is off. This message applies to data ports that act as DCEs.	Examine the attached DTE and cable connected to the system's port. ■ Check that the port cable is securely attached at both ends. ■ Check the status of the attached equipment.
EER at Network 1	The error rate of the received network signal exceeds the currently configured threshold. This condition only occurs if the network interface is configured for ESF framing. This condition clears when the error rate falls below the threshold value, which may take up to 15 minutes.	■ Verify that the network cable is securely attached at the network interface. ■ Contact your network provider.
Ethernet Link Down	The communication link for the Ethernet port is down and the Interface Status for the port is enabled.	Check the LAN connected to the Ethernet port.

Table 6-1. Alarm Conditions (2 of 3)

Alarm Condition	What It Indicates	What To Do
LOS at Network 1	A Loss of Signal (LOS) condition is detected on the network interface. Clears when the ratio of ones to zeros received is greater than or equal to 12.5%.	
	■ Network cable problem.	■ Check that the network cable is securely attached at both ends.
	■ No signal is being transmitted at the far-end DSU/CSU.	■ Check far-end DSU/CSU status.
	■ T1 facility problem.	■ Contact your network provider.
Network Com Link Down	The communication link for the COM port is down and the COM port is configured for Net Link.	Check the router connected to the COM port.
OOF at Network 1	An Out of Frame (OOF) condition is detected on the network interface.	
	■ Incompatible framing format between the network and the DSU/CSU.	■ Check that the framing format for the network interface is correct.
	■ Network cabling problem.	■ Check that the network cable is securely attached at both ends.
	■ T1 facility problem.	■ Contact your network provider.
Primary Clock Failed	A failure of the configured primary clock source for the unit was detected and the secondary clock is providing the timing for the unit. This condition clears when the configured primary clock is restored.	■ Check that the network cable is securely attached at both ends. ■ Contact your network provider.
Self-Test Failure	The unit did not pass its basic verification tests when it was powered on or reset.	■ Reset the unit. ■ Contact your service representative.
Two Level-1 Users Accessing Device	Another user with Level-1 security access is currently accessing the unit. Be aware that actions of the other user may override your test commands and configuration changes.	Wait until no other Level-1 users are accessing the unit if testing or configuration will be performed.

Table 6-1. Alarm Conditions (3 of 3)

Alarm Condition	What It Indicates	What To Do
Yellow at Network 1	A yellow alarm signal is received on the network interface.	
	■ Network cable problem.	■ Check that your network cable is securely attached at both ends.
	■ T1 facility problem.	■ Contact your network provider.

Troubleshooting Device Problems

The unit is designed to provide many years of trouble-free service. However, if a problem occurs, refer to Table 6-2, Device Problems, for possible solutions.

Table 6-2. Device Problems

Symptom	Possible Cause	Solutions
No power, or the LEDs are not lit.	The power cord is not securely plugged into the wall receptacle to rear panel connection.	Check that the power cord is securely attached at both ends.
	The wall receptacle has no power.	■ Check the wall receptacle power by plugging in some equipment that is known to be working. ■ Check the circuit breaker. ■ Verify that your site is not on an energy management program.
Power-On Self-Test fails. Only Alarm LED is on after power-on.	The unit has detected an internal hardware failure.	■ Reset the unit and try again. ■ Contact your service representative. ■ Return the unit to the factory (refer to *Warranty, Sales, Service, and Training Information* on page A of this document).
Cannot access the unit or the menu-driven user interface.	Login or password is incorrect, COM port is misconfigured, or the unit is otherwise configured so it prevents access.	■ Reset the unit (see *Restoring Communication with an Improperly Configured Unit* on page 6-4.) ■ Contact your service representative.
Failure *xxxxxxxx* appears at the top of the System and Test Status screen, at Self-Test Results.	The unit has detected an internal software failure.	■ Record the 8-digit code from the System and Test Status screen. ■ Reset the unit and try again. ■ Contact your service representative and provide the 8-digit failure code.
An LED appears dysfunctional.	LED is burned out.	Run the Lamp Test. If the LED in question does not flash with the other LEDs, then contact your service representative.
Not receiving data.	Network cable loose or broken.	■ Reconnect or repair the cable. ■ Call the network service provider.

Tests Available

The following tests are available to the 7123 DSU/CSU.

Test Menu Example

```
main/test                                                          7123
Device Name: Node A                                  09/09/2001 06:01

                                    TEST

                              Network Physical Tests
                              Data Port Physical Tests

                              IP Ping
                              Lamp Test

                              Abort All Tests









--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
```

Tests can be commanded from the OpenLane SLM system using its enhanced Diagnostic Troubleshooting graphical interface, as well as from the menu-driven user interface.

Test Timeout Feature

A Test Timeout feature is available to automatically terminate a test (as opposed to manually terminating a test) after it has been running a specified period of time.

To use this feature, enable the Test Timeout configuration option, and set a duration for the test to run in the Test Duration (min) configuration option (see *Configuring General System Options* in Chapter 3, *Configuration*).

NOTE:

These configuration options do not pertain to tests commanded by the DTE, like a DTE-initiated External Loopback.

Starting and Stopping a Test

Use this procedure to start, monitor, or abort specific tests. To abort all active tests on all interfaces, see *Aborting All Tests* on page 6-11.

When the status of a test is . . .	The only command available is . . .
Inactive	Start
Active	Stop

Start or stop an individual test using the same procedure.

▶ Procedure

To start and stop a loopback or pattern test:

1. Follow this menu selection sequence:

   Main Menu → *Test*

2. Select Network Physical Tests or Data Port Physical Tests and press Enter.

   The selected test screen appears. **`Start`** appears in the Command column. **`Inactive`** appears in the Status column.

3. Highlight the **`Start`** command for the test you want to start and press Enter.

   `Stop` now appears and is highlighted, and the status of the test changes to **`Active`**.

4. Press Enter to stop the test.

   `Start` reappears and the status of the test changes back to **`Inactive`**.

5. View the length of time that the test has been running in the Result column.

Aborting All Tests

Use the Abort All Tests selection from the Test menu to abort all tests running on all interfaces, with exception to DTE-initiated loopbacks. To abort individual tests that are active, see *Starting and Stopping a Test* on page 6-10.

▶ Procedure

To abort all tests on all interfaces:

1. Follow this menu selection sequence:

   Main Menu → *Test*

2. Select Abort All Tests and press Enter.

   `Command Complete` appears when all tests on all interfaces have been stopped.

   NOTE:

   Abort All Tests does not interrupt DTE-initiated loopbacks.

Physical Tests

A 7123 DSU/CSU's physical tests screen for the network interface is shown below.

Main Menu → Test → [Network Physical Tests/Data Port Physical Tests]

Physical Tests Screen Example

```
main/test/network                                                    7123
Device Name: Node A                                    09/09/2001 06:02

                          NETWORK 1 PHYSICAL TESTS

Test                          Command     Status     Results

 Local Loopbacks
   Line Loopback:              Start       Inactive   0:00:00
   Payload Loopback:           Start       Inactive   0:00:00

 Remote Loopbacks
   Send Line Loopback: Down    Send        Inactive   0:00:00

 Pattern Tests
   Send:    user-defined 0a0a  Stop        Active     0:00:00 - Errors 99999+
   Monitor: user-defined 0a0a  Stop        Active     0:00:00 - Errors 99999+



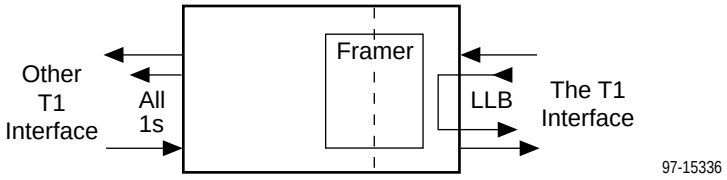

--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
 InjectERR    ResetMon
```

The ResetMon function key at the bottom of the screen only appears when a Monitor 511 test pattern is Active. Select ResetMon to reset the monitor pattern error counter.

Line Loopback

The local Line Loopback (LLB) loops the information received on the selected interface back to the source of the loopback. When used with a pattern test at the remote node, LLB determines whether the problem is with the sending device or the T1 facility.

Main Menu → Test → Network Physical Tests



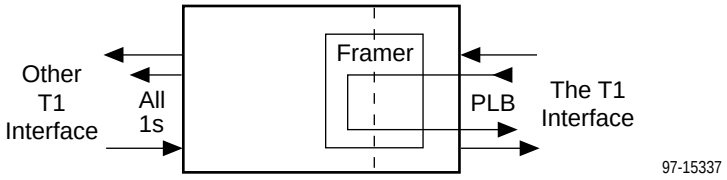
An LLB cannot be started when one of the following tests is active:

- Payload Loopback, Send Remote Line Loopback, or an active Monitor Pattern on this network interface.
- Send Pattern test on this network interface.

Payload Loopback

The local Payload Loopback (PLB) loops the information received on the selected interface back to the network after it has passed through the receive and transmit framing section of the device. Use the PLB to determine whether the problem is with the T1 facility or in the circuitry of the remote device.

Main Menu → Test → Network Physical Tests



A PLB cannot be started when one of the following tests is active:

- Line Loopback, Repeater Loopback, Send Remote Line Loopback, or an active Monitor Pattern on this network interface.
- Send Pattern test on this network interface.

Send Line Loopback

The remote Line Loopback (LLB) up and down codes are in-band codes that allow control of a remote device. The LLB Up code invokes a line loopback in the remote unit while the LLB Down code terminates the remote line loopback. Network loopbacks are defined in AT&T TR 62411.

Main Menu → Test → Network Physical Tests

A remote LLB cannot be started when one of the following tests is active:

- Any Loopback on the same interface.
- Send FT1 Loopback or Data Channel Loopback on the synchronous data port.

▶ Procedure

To start and stop a remote Line Loopback:

1. Select Network Physical Tests.

   Main Menu → Test → Network Physical Tests

2. Select the code Up or Down in the Send Line Loopback field.
   - **Up:** Puts a remote device in loopback.
   - **Down:** Takes the remote device out of loopback.
3. Highlight Send and press Enter to start the test. The code is sent for 10 seconds.
4. View the length of time that the test has been running in the Result column.

Send and Monitor Pattern Tests

The pattern tests enable a DSU/CSU to either send or monitor a known bit pattern. These tests generate industry-standard bit patterns that can be used to determine whether information is being correctly transmitted across a circuit.

The following test patterns are available:

— **QRSS**	— **511**
— All-zeros	— 2047
— All-ones	— 2E15-1 (215-1)
— 1-in-8	— 2E20-1 (220-1)
— 3-in-24	— User-defined 2-byte test pattern (a0a0)
— 63	

A Send Pattern test cannot be started when any loopback is running on the same interface.

▶ Procedure

To send and monitor a Pattern Test:

1. Select Network Physical Tests.

   Main Menu→ Test→Network Physical Tests

2. Select the desired pattern in the Send or Monitor field. If sending/monitoring a user-defined pattern, enter the desired 2-byte hexadecimal value in the field next to Send or Monitor.

   When sending a pattern, the Inject ERR function key appears. Use Inject ERR if you want to inject a bit error in the transmitted bit pattern.

3. Highlight the Send command to send a pattern, or the Start command to monitor a pattern, and press Enter to start the test or start monitoring it.

4. View the length of time that the test has been running in the Results column. An error count is also displayed. When monitoring a pattern, the ResetMon virtual function key appears. ResetMon resets the error count to zero.

5. Highlight Stop and press Enter to stop the test.

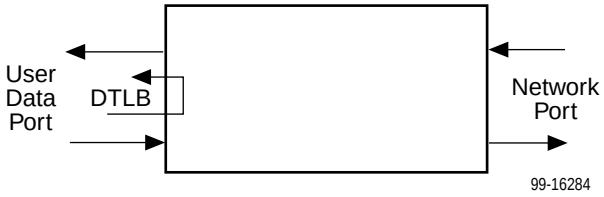
6. View the length of time that the test has been running in the Result column.

DTE Loopback

The local DTE external Loopback (DTLB) test loops the received signal on the DTE interface back to the DTE. Use this test to isolate problems on the user data port.

Main Menu → Test → Data Port Physical Tests

An attached device or test equipment must generate the data to be looped back.



CAUTION:

Any IP data being sent while this test is active will be disrupted.

IP Ping Test

An IP Ping test can be run to test connectivity between the DSU/CSU and any NMS to which it has a route.

Times when you might want to run an IP Ping test are:

- To verify the entire path between a newly installed remote site DSU/CSU and the central site NMS. During a remote site installation, an IP Ping test is typically run from the remote site to ping the NMS at the central site. The remote DSU/CSU must have SNMP trap managers configured, and one of those trap managers must be the central site NMS.
- To test the path to the NMS trap managers during installation of the central site DSU/CSU. The remote DSU/CSU must have configured the SNMP trap managers to be sent the ping.

▶ Procedure

To ping the NMS at the central site:

1. Verify that the central site NMS has the DSU/CSU's IP address in its routing table so it can communicate with the DSU/CSU.
2. Verify that the central site NMS's router has the DSU/CSU's IP address in its routing table so it can communicate with the DSU/CSU.
3. Verify that the central site NMS has been configured as an SNMP Trap Manager if the router is to route data, so a route has been configured within the DSU/CSU.

   Main Menu → Configuration → Management and Communication → SNMP Traps

4. Select the IP Ping test.

   Main Menu → Test → IP Ping

5. Enter the IP Address of the central site NMS, then select Start.
6. Verify the results of the IP Ping test.
   - — While the test is running, **`In Progress...`** appears in the Status field.
   - — When the test is finished, **`Alive. Latency =`** *nn* **`ms`** should appear as the Status (*nn* being the amount of time the test took in milliseconds).

     If any other message is displayed, additional testing will be required.

Lamp Test

The DSU/CSU supports a Lamp Test to verify that all LEDs are lighting and functioning properly. All LEDs flash or blink on and off at the same time every 0.5 seconds during execution of the test. When the test is stopped, the LEDs are restored to their normal condition.

Main Menu → *Test* → *Lamp Test*

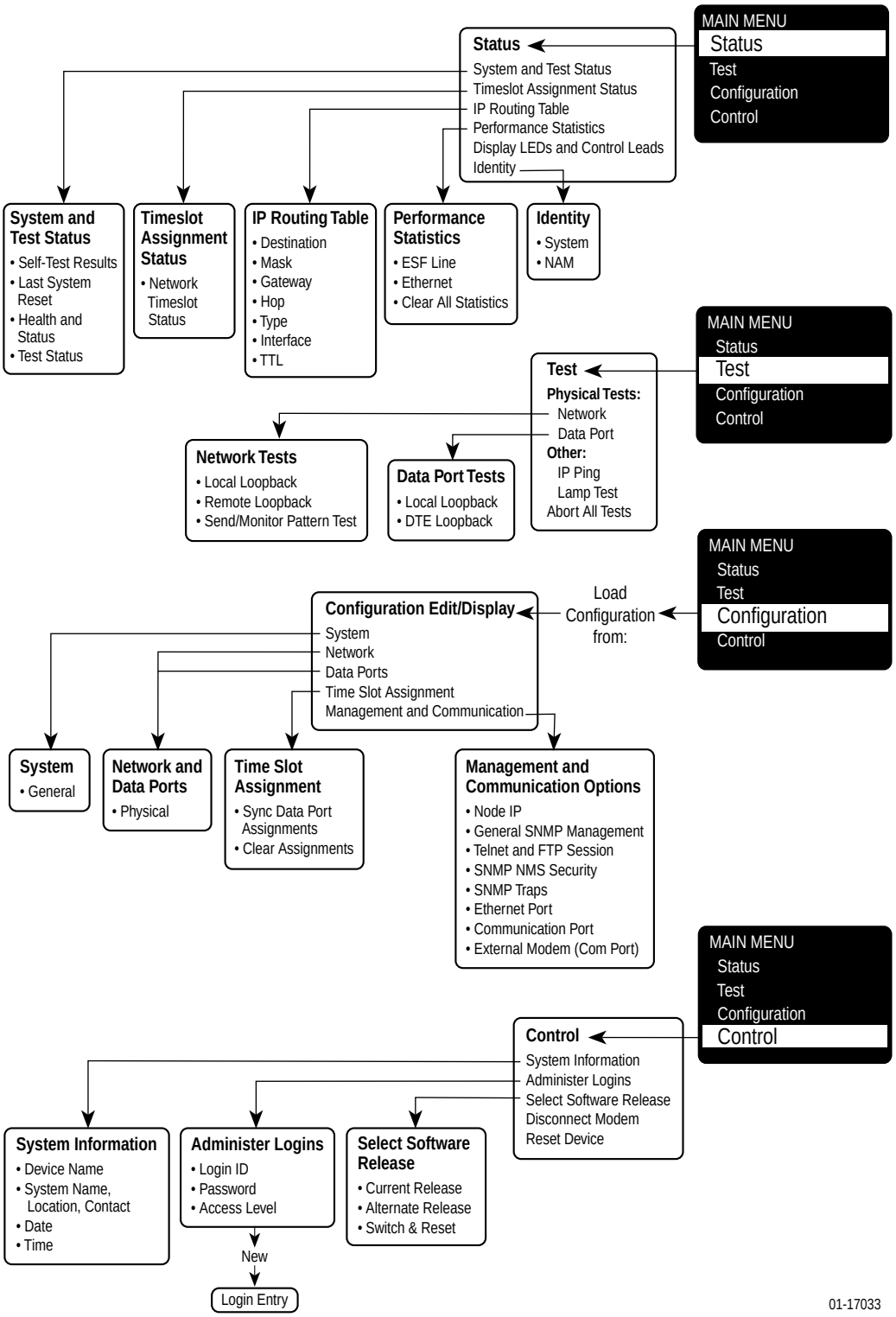
If the Test Timeout configuration option is enabled and a Test Duration is set, the Lamp Test stops when the test duration expires. See *Test Timeout Feature* on page 6-10 for additional information.

Menu Hierarchy

A

Menus

The following menus are a graphical representation of the 7123 SNMP DSU/CSU's menu organization.


MAIN MENU
Status
Test
Configuration
Control
Status
System and Test Status
Timeslot Assignment Status
IP Routing Table
Performance Statistics
Display LEDs and Control Leads
Identity
System and Test Status
• Self-Test Results
• Last System Reset
• Health and Status
• Test Status
Timeslot Assignment Status
• Network Timeslot Status
IP Routing Table
• Destination
• Mask
• Gateway
• Hop
• Type
• Interface
• TTL
Performance Statistics
• ESF Line
• Ethernet
• Clear All Statistics
Identity
• System
• NAM
MAIN MENU
Status
Test
Configuration
Control
Test
Physical Tests:
Network
Data Port
Other:
IP Ping
Lamp Test
Abort All Tests
Network Tests
• Local Loopback
• Remote Loopback
• Send/Monitor Pattern Test
Data Port Tests
• Local Loopback
• DTE Loopback
MAIN MENU
Status
Test
Configuration
Control
Load Configuration from:
Configuration Edit/Display
System
Network
Data Ports
Time Slot Assignment
Management and Communication
System
• General
Network and Data Ports
• Physical
Time Slot Assignment
• Sync Data Port Assignments
• Clear Assignments
Management and Communication Options
• Node IP
• General SNMP Management
• Telnet and FTP Session
• SNMP NMS Security
• SNMP Traps
• Ethernet Port
• Communication Port
• External Modem (Com Port)
MAIN MENU
Status
Test
Configuration
Control
Control
System Information
Administer Logins
Select Software Release
Disconnect Modem
Reset Device
System Information
• Device Name
• System Name, Location, Contact
• Date
• Time
Administer Logins
• Login ID
• Password
• Access Level
New
Login Entry
Select Software Release
• Current Release
• Alternate Release
• Switch & Reset
01-17033

SNMP MIBs and Traps

B

This appendix contains the following:

- *MIB Support* on page B-2
- *Downloading MIBs and SNMP Traps* on page B-2
- *System Group (mib-2)* on page B-3
  - *DSU/CSU's sysDescr (system 1)*
  - *DSU/CSU's sysObjectID (system 2)*
- *Interfaces Group (mib-2)* on page B-4
  - *Paradyne Indexes to the Interface Table (ifTable)*
- *Standards Compliance for SNMP Traps* on page B-4
  - *Trap: warmStart*
  - *Trap: authenticationFailure*
  - *Traps: linkUp and linkDown*
  - *Traps: enterprise-Specific*

MIB Support

The 7123 SNMP DSU/CSU supports the SNMP Version 1, and has the capability of being managed by any industry-standard SNMP manager and accessed by external SNMP managers using the SNMP protocol.

The following MIBs are supported:

- MIB II (RFC 1213 and RFC 1573)
- RS-232-Like MIB (RFC 1659)
- Enterprise MIB

Downloading MIBs and SNMP Traps

Paradyne standard and enterprise MIBs are available from the Paradyne World Wide Web site.

▶ Procedure

To access Paradyne MIBs:

1. Access the Paradyne World Wide Web site at **www.paradyne.com**.
2. Select Technical Support.
3. Select Management Information Base (MIBs).

The download procedure may vary depending upon your browser or NMS application software. Refer to your browser or NMS manual for additional download information.

System Group (mib-2)

This section provides the system description and system object identifier for the System Group for the 7123 DSU/CSU, which is an SNMPv1 MIB.

DSU/CSU's sysDescr (system 1)

The following is the system description (sysDescr [system 1]) for the NMS subsystem in the 7123 DSU/CSU:

> PARADYNE T1 DSU/CSU; Model: 7123; S/W Release: *(MM.mm.bb [MM=Major.mm=minor.bb=build] format)*; NAM CCA number: *(hardware version in hhhh-hhh format)*; Serial number: *sssssss*

DSU/CSU's sysObjectID (system 2)

The following is the system object identifier (sysObjectID [system 2]), or OID, for the NMS subsystem in the 7123 DSU/CSU:

> 1.3.6.1.4.1.1795.1.14.2.4.12.1

Interfaces Group (mib-2)

Clarification for objects in the Interfaces Group, as defined in RFC 1573 and RFC 1213, which is an SNMPv1 MIB, is provided in this section.

Paradyne Indexes to the Interface Table (ifTable)

Table B-1, Paradyne Interface Objects Information, provides the ifName for each interface type, the ifDescr, and the ifIndex that Paradyne has assigned to each.

Table B-1. Paradyne Interface Objects Information

ifName	Description	ifDescr (ifEntry 2)	ifIndex
Physical Layer			
Network T1	T1 network interface	Network T1; T1 DSU/CSU; Hardware Version: *hhhh-hhh*	101001001
Ethernet	Ethernet Port	Ethernet Port; T1 DSU/CSU; Hardware Version: *hhhh-hhh*	101006001
Sync Data Port S01P1	Synchronous Data Port-1	Synchronous Data Port, Slot: 1, Port: 1; T1 DSU/CSU; Hardware Version: *hhhh-hhh*	101003001
COM	Communications port	COM Port; T1 DSU/CSU; Hardware Version: *hhhh-hhh*	101004001

Standards Compliance for SNMP Traps

This section describes the DSU/CSU's compliance with SNMP format standards and with its special operational trap features.

The unit supports the following:

- *Trap: warmStart*
- *Trap: authenticationFailure*
- *Traps: linkUp and linkDown*
- *Traps: enterprise-Specific*

These traps are listed in alphabetical order within each table.

Trap: warmStart

This trap indicates that the DSU/CSU has been reset and has stabilized.

Table B-2. warmStart Trap

Trap	What It Indicates	Possible Cause
warmStart	DSU/CSU has just reinitialized and stabilized itself.	■ Reset command sent. ■ Power disruption. *String:* 'Unit reset.'
	Variable-Binding	
	devLastTrapString (devHealthAndStatus.mib)	

Trap: authenticationFailure

This trap indicates that access to the DSU/CSU was unsuccessful due to lack of authentication.

Table B-3. authenticationFailure Trap

Trap	What It Indicates	Possible Cause
authenticationFailure	Access to the DSU/CSU was attempted and failed.	■ SNMP protocol message not properly authenticated. ■ Three unsuccessful attempts were made to enter a correct login user ID/password combination. ■ IP Address security is enabled and a message was received from the SNMP Manager whose address was not on the lost of approved managers. *String:* 'Unauthorized access attempted.'
	Variable-Binding	
	devLastTrapString (devHealthAndStatus.mib)	

Traps: linkUp and linkDown

These traps are supported on the physical sublayer interfaces: network, Ethernet, and synchronous data ports.

Table B-4. linkUp and linkDown Traps

Trap	What It Indicates	Possible Cause
linkDown	A failure in one of the communication interfaces has occurred.	A failure in one of the communication interfaces has occurred.
linkUp	One of the failed communication interfaces is up and operational.	One of the failed communication interfaces is up and operational.

Their linkUp and linkDown variable-bindings are in Table B-5, linkUp and linkDown Variable-Bindings.

Physical and logical sublayers are represented by the entry in the MIB II Interfaces Table.

Table B-5. linkUp and linkDown Variable-Bindings (1 of 2)

Interface	Variable-Bindings	Possible Cause
Physical Sublayer		
Network (Supported by the media-specific DS1 MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – One or more alarm conditions are active on the interface. Alarm conditions include: – Loss of Signal (LOS) or far-end loss of signal – Out of Frame (OOF) – Alarm Indication Signal (AIS) – Excessive Error Rate (EER) – Yellow Alarm *Strings:* '$ifString down.' No alarms exist. (e.g., 'Network T1 down due to yellow alarm.') '$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – No alarms on the interface. *String:* '$ifString up.'
Synchronous Data Port (Supported by the media-specific RS232-like MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – One or more alarm conditions are active on the port. Alarm conditions include: – DTR off [1] – RTS off [2] – ' ' – Not DTR or RTS, but link is down. *String:* '$ifString $alarmString down.' (e.g., 'Sync Data Port S01P1 DTR and RTS down.') '$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – No alarms on the port. *String:* '$ifString up.'

[1] The DTR alarm condition will only generate a linkUp/linkDown trap if the DTE supports the DTR lead state.

[2] The RTS alarm condition will only generate a linkUp/linkDown trap if the DTE supports the RTS lead state.

[3] A linkUp/linkDown trap is based solely upon whether the interface is enabled or disabled.

Table B-5. linkUp and linkDown Variable-Bindings (2 of 2)

Interface	Variable-Bindings	Possible Cause
Physical Sublayer *(cont'd)*		
Ethernet Port	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – Communication is not possible over the Ethernet port. *Strings:* '$ifString down.' '$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – Communication on the port is restored. *String:* '$ifString up.'

1 The DTR alarm condition will only generate a linkUp/linkDown trap if the DTE supports the DTR lead state.

2 The RTS alarm condition will only generate a linkUp/linkDown trap if the DTE supports the RTS lead state.

3 A linkUp/linkDown trap is based solely upon whether the interface is enabled or disabled.

Traps: enterprise-Specific

These traps indicate that an enterprise-specific event has occurred. Supported enterprise-specific traps are listed below.

Table B-6. enterprise-Specific Traps and Variable-Bindings

Trap	Variable-Bindings	Possible Cause
enterpriseConfig-Change(6)	■ devLastTrapString (devHealthAndStatus.-mib)	Configuration has been changed via the menu-driven user interface, an SNMP Manager, or auto-configuration after 60 seconds has elapsed without another change. *String:* 'Device configuration change.'
enterprisePrimary-ClockFail(1)	■ devLastTrapString (devHealthAndStatus.-mib)	Operating software has detected that the primary clock source has failed. *String:* 'Primary clock failed.'
enterprisePrimary-ClockFailClear(101)		Operating software has detected that the primary clock source is operational again. *String:* 'Primary clock restored.'
enterpriseSelfTest-Fail(2)	■ devLastTrapString (devHealthAndStatus.-mib)	Unit has completed (re)initialization and a hardware failure was detected. *String:* 'Self test failed: $*s*.' ($*s* is the contents of devSelfTestResult.)
enterpriseTest-Start(5)	For physical interfaces: ■ ifIndex (RFC 1573) ■ .0.0 (placeholder) ■ devLastTrapString (devHealthAndStatus.-mib	At least one test has been started on an interface. *String:* '$testString test started on $ifString.' (e.g., 'DTE Loopback test started on Sync Data Port S01P1.')

Physical Interface Alarm Defaults

This alarm only applies to the DSU/CSU's network interface.

Table B-7. Network Physical Interface Alarm Defaults

Item	Sample Type[1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Unavailable Seconds	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devTelcoFreeRunUAS *OID:*.1.3.6.1.4.1.1795.2.24.2.6**.-**5.4.8.1.2**.I**	900 secs (15 mins)	Rising	1	1

[1] D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB.

[2] **I** in the OID = Interface ID of the link.

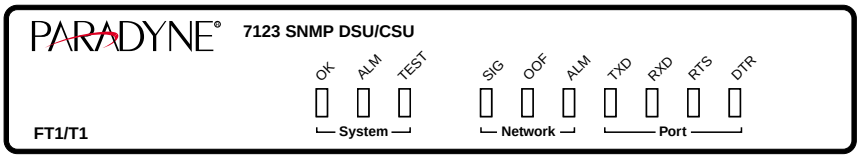
Connectors, Cables, and Pin Assignments

C

This appendix shows the DSU/CSU's front and rear panels, and the pin assignments for the connectors/interfaces and cables.

Front Panel

The following illustration shows the 7123 SNMP DSU/CSU's front panel.

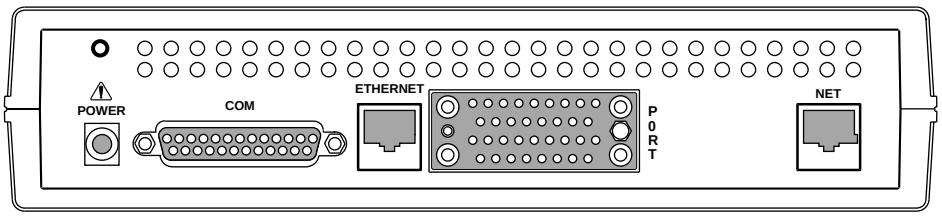


01-17031

See *Viewing LEDs and Control Leads* in Chapter 5, *Operation and Maintenance* for information about the front panel LEDs.

Rear Panel

The following illustration shows the 7123 SNMP DSU/CSU's rear panel.



00-16690

The sections that follow provide pin assignments for each interface.

NOTE:

In the pin assignment tables of this appendix, if the pin number is not shown, it is not being used.

T1 Network Interface

The T1 network interface/connector is an RJ48C 8-position keyed modular jack.

T1 Network Cable (Feature No. 3100-F1-500)

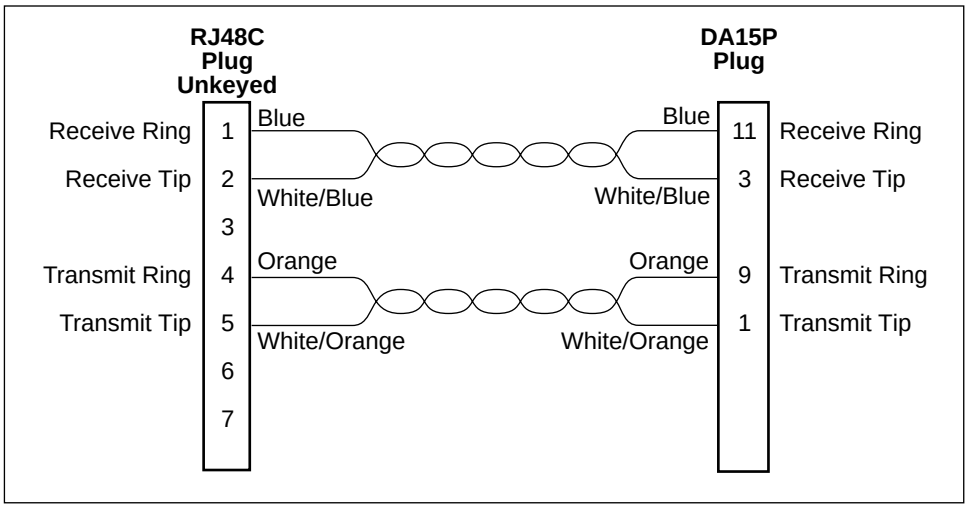
Network access is via a 20-foot cable with an RJ48C unkeyed plug-type connector on each end. The following table shows pin assignments and the purpose of each.

Function	Circuit	Direction	Pin Number
Receive Ring	R1	From Network	1
Receive Tip	T1	From Network	2
Transmit Ring	R	To Network	4
Transmit Tip	T	To Network	5

This cable comes with the DSU/CSU.

Canadian T1 Line Interface Cable (Feature No. 3100-F1-510)

The T1 line interface cable is used in Canada as an interface between the DSU/CSU's network connector and the T1 network interface. The following shows pin assignments and the purpose of each.



98-16215

COM Port Connector

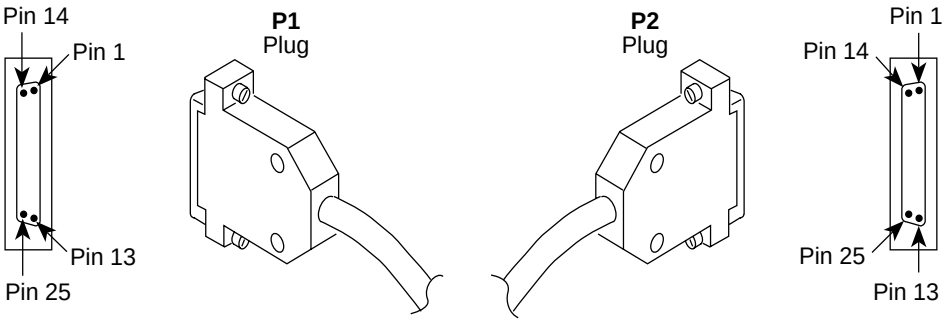
The following table provides the pin assignments for the DSU/CSU's 25-position EIA-232-C communication port connector.

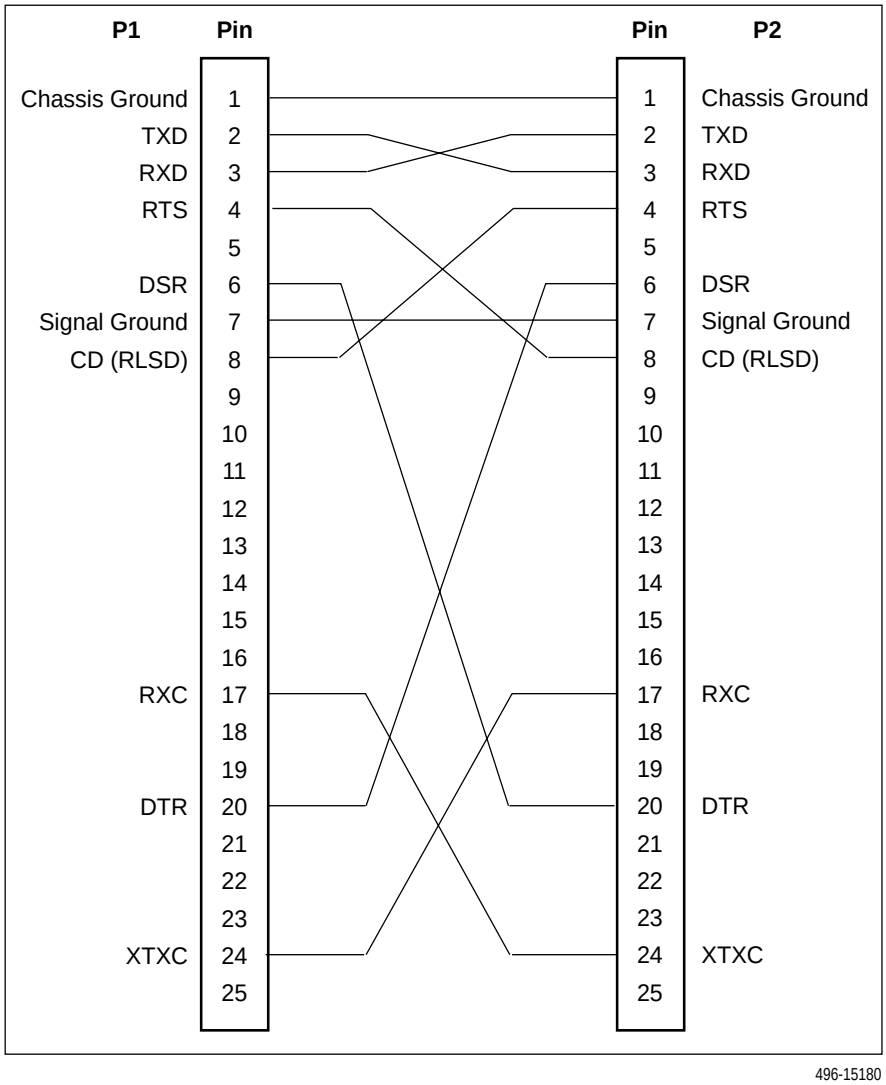
Signal	Direction	Pin #
Shield (GND)	—	1
DCE Transmit Data (TXD)	From DTE (In)	2
DCE Receive Data (RXD)	To DTE (Out)	3
DCE Request To Send (RTS)	From DTE (In)	4
DCE Clear To Send (CTS)	To DTE (Out)	5 *
DCE Data Set Ready (DSR)	From DTE (In)	6 *
Signal Ground (GND)	—	7
DCE Carrier Detect (CD)	To DTE (Out)	8 *
DCE Data Terminal Ready (DTR)	From DTE (In)	20

* Pins 5, 6, and 8 are tied together.

Standard EIA-232-D Crossover Cable

A standard crossover cable can be used to connect the COM port to an external modem. The external modem must be configured so it is compatible with the DSU/CSU. See the procedure in *Configuring an External Modem* on page C-5 to configure an external modem.





496-15180

Configuring an External Modem

▶ Procedure

To configure an external modem:

1. Disconnect the asynchronous terminal from the standard cable. See *Standard EIA-232-D Crossover Cable* on page C-4 for an illustration of the COM Port connection.
2. Reconnect the crossover cable to the external modem.
3. Enable auto-answer on your modem, and configure it to use the following LSD, DSR, CTS, RTS, and DTR control leads.

   See the table below for AT D0 command strings. Use the following command string:

   AT &C0 &D2 &S0 &R1 \D0 S0=1

AT Command String	To configure the modem to . . .
&C0	Force LSD on.
&D2	Drop the connection when the unit drops DTR.
&S0	Force DSR on.
&R1	Ignore RTS.
\D0	Force CTS on.
S0=1	Automatically answer incoming calls.

Data Port Connector

The following table provides the pin assignments for the 34-position V.35 connector to the DTE.

Signal	ITU CT#	Direction	34-Pin Socket
Shield	101	—	A
Signal Ground/Common	102	—	B
Request to Send (RTS)	105	To DSU (In)	C
Clear to Send (CTS)	106	From DSU (Out)	D
Data Set Ready (DSR)	107	From DSU (Out)	E
Receive Line Signal Detector (RLSD or LSD)	109	From DSU (Out)	F
Data Terminal Ready (DTR)	108/1, /2	To DSU (In)	H
Local Loopback (LL)	141	To DSU (In)	L
Transmit Data (TXD)	103	To DSU (In)	P (A) S (B)
Receive Data (RXD)	104	From DSU (Out)	R (A) T (B)
Transmit Signal Element Timing – DTE Source (XTXC or TT)	113	To DSU (In)	U (A) W (B)
Receive Signal Element Timing – DCE Source (RXC)	115	From DSU (Out)	V (A) X (B)
Transmit Signal Element Timing – DCE Source (TXC)	114	From DSU (Out)	Y (A) AA (B)
Test Mode Indicator (TM)	142	From DSU (Out)	NN

Standard V.35 Straight-through Cable

A standard V.35 straight-through cable can be used to connect a DTE port to a DTE, where a 34-pin plug-type connector is needed for the data port and a 34-position socket-type connector is needed for the DTE. No special-order cables are required.

Ethernet Port Connector

The following table provides the pin assignments for the DSU/CSU's 8-position RJ45 Ethernet port unkeyed modular jack.

Signal	Direction	Pin #
10BaseT Transmit Data (TD+)	To LAN Interface (Out)	1
10BaseT Transmit Data (TD–)	To LAN Interface (Out)	2
10BaseT Receive Data (RD+)	From LAN Interface (In)	3
10BaseT Receive Data (RD–)	From LAN Interface (In)	6

Technical Specifications

D

Table D-1. 7123 SNMP DSU/CSU Technical Specifications (1 of 2)

Specification	Criteria
Approvals	
FCC Part 15	Class A digital device.
FCC Part 68	Refer to the equipment's label for the Registration Number.
Industry Canada	Refer to the equipment's label for the Certification Number.
Safety	Refer to the equipment's label for safety information.
Physical Environment	
Operating temperature	32°F to 122°F (0°C to 50°C)
Storage temperature	–4°F to 158°F (–20°C to 70°C)
Relative humidity	5% to 85% (noncondensing)
Shock and vibration	Withstands normal shipping and handling
Power Consumption and Dissipation	4.5 watts, 60 Hz ± 3, 0.135 A at 120 VAC±12 Result: 15.4 Btu per hour
Physical Dimensions	
Height (with feet) Height (without feet)	2.1 inches (5.3 cm) 2.0 inches (5.1 cm)
Width	6.2 inches (15.7 cm)
Depth	8.7 inches (22.1 cm)
Weight	1.38 lbs (0.62 kg)
COM Port	25-position (DB25) connector
Standard	EIA-232/ITU, V.24 (ISO 2110)
Data rates	9.6, 14.4, 19.2, 28.8, 38.4, 57.6, and 115.2 Kbps

Table D-1. 7123 SNMP DSU/CSU Technical Specifications (2 of 2)

Specification	Criteria
T1 Network Interface	8-position modular unkeyed USOC RJ48C jack
Data rates	Up to 1.536 Mbps
Services supported	Fractional T1
Physical interface (USA)	RJ48C
Physical interface (Canada)	CA81A using adapter cable
Framing format	D4, ESF
Coding format	AMI, B8ZS
Line Build-Out (LBO)	0.0 dB, –7.5 dB, –15 dB, –22.5 dB
ANSI PRM	Selectable
Bit stuffing	AT&T TR 62411
Ethernet Port	8-position modular unkeyed USOC RJ45 jack
Standard	ANSI/IEEE Standard 802.3, Ethernet Version 2
Data rates	10/100 BaseT (auto-sensing 10 and 100 Mbps Ethernet rates)
Data Port	34-position V.35 connector
Standard	V.35/ITU (ISO 2593)
Data rates	Variations for T1 rates; automatically set to the network rate.

Equipment List

E

Equipment

See *Cables* on page E-2 for cables you can order.

Description	Model/Feature Number
7123 SNMP DSU/CSU	
7123 SNMP DSU/CSU *Includes 1-Slot Housing, 120 Vac Power Supply, Network Cable, and Installation Instructions.*	7123-A1-201
User Manual	
7123 SNMP DSU/CSU User's Guide (Paper Manual)	7123-A2-GB20
NMS Products	
OpenLane SLM Enterprise	7805-D1-001
OpenLane SLM Workgroup	7805-D1-003

Cables

This table lists cables you can order.

Description	Part Number	Feature Number
RJ48C T1 Network Cable, RJ48C-to-RJ48C/RJ49C (20 feet / 6.1 meters) – *For use in the U.S.*	035-0209-2031	3100-F1-500
T1 Line Interface Cable, RJ48C-to-CA81A (20 feet / 6.1 meters) – *For use in Canada.*	035-0221-2031	3100-F1-510
Standard EIA-232 Straight-Through Cable, DB25-to-RJ48 (14 feet / 4.3 meters) – *For connection to an asynchronous terminal or PC with an 8-pin modular interface.*	035-0314-1431	3100-F2-540
Standard EIA-232 Straight-Through Cable, DB25-to-D-Sub9 (14 feet / 4.3 meters) – *For connection to a PC with a D-Sub9 interface.*	035-0313-1431	3100-F2-550
V.35 DTE Adapter, EIA-530-A-to-V.35 – *For connection to equipment with V.35, MS34 connectors.*	035-0244-0031	3100-F1-570
Standard EIA-232-D Crossover Cable (14 feet / 4.3 meters) – *For connection to an external device.*	035-0336-1431	9008-F1-550

Index

A

aborting tests, 6-11
Access
  Dial-In, 3-36
  Name, 3-21
  Type, 3-26
Access Level, 4-9–4-10
  assigning, 4-8
  Port, 3-33
  security, 2-1
  Session, 3-23
AIS
  alarm condition, 6-5
  LED, 5-4–5-5
  linkDown trap, B-7
Alarm, 6-5
  (Fail), 5-4
  conditions, 6-5
  LED is lit, 6-8
ALM LED, 5-4–5-5
Alternate software revision, 5-2
ANSI Performance Report Messages, 3-11
assign
  community names and access levels, 4-8
  synchronous data port, 3-17
  time slots and cross connections, 3-16
AT commands, 3-36
authentificationFailure trap, B-5
AutoRoute, 3-28

B

back door access when locked out, 6-4
Backspace, 2-6
blank field value, 2-9
branches/menus, 2-4

C

changing
  configuration options, 3-5
  software release, 5-26
Character
  Length, 3-32
  matching, 2-9
Circuit Identifier, 3-12
Clearing
  cross connection assignments, 3-16
  existing information, 3-7
  statistics, 5-18
Clock
  Invert Transmit, 3-13
  setting system, 3-7
  Source, 3-9
    Transmit, 3-13
COM port, 3-20, 3-28, 3-36
  connector, C-3
Communication Port
  user interface options, 3-32
Community Name, 3-21
  assigning, 4-8
Configuration
  displaying and changing options, 3-4
  menu, 3-2
  menu/branch, 2-4
  option areas, 3-3
  saving options, 3-6
  tables, 3-3
configuring
  network interface, 3-10
  System options, 3-9
  the system, 3-2
Control
  keys, 2-6
  Leads
    and LEDs, 5-3
    Ignore, 3-33
  menu/branch, 2-4
controlling
  asynchronous terminal access, 4-2
  external device access, 4-4
  FTP access, 4-4
  SNMP access, 4-7
  Telnet access, 4-4
creating a login, 4-10
cross connections, 3-16
crossover EIA-232 cable, C-4
CTS
  down, 6-5
  down to Port Device, 5-12
current software revision, 5-2

D

Data
  Port
    physical options, 3-13
  port connector pin assignments, C-6
  Rate (Kbps), 3-32
  selection criteria, 2-1
Data Channel Loopback
  Network-Initiated, 3-15
Date & Time setting, 3-7
DDS Line statistics, 5-22
Default IP Destination, 3-20
deleting a login, 4-11
Destination, 3-28
  Default IP, 3-20
Device
  messages, 5-6
  troubleshooting problems, 6-8
Dial-In Access, 3-36
disabling SNMP access, 4-7
Disconnect Time (Minutes), 3-23, 3-34
displaying
  configuration options, 3-4
  identity information, 5-2
  LEDs and control leads, 5-3
downloading
  determining when completed, 5-26
  MIBs and SNMP traps, B-2
  software, 5-23, 5-25
DTE
  Loopback, 6-17
  port connector pin assignments, C-6
  port-initiated loopbacks, 3-14
DTLB, 6-17
DTR
  down, 6-5
  down from Port-1 Device, 5-12
  Ignore Control Leads, 3-33

E

EER
  at Network, 5-12, 6-5
  LED, 5-4–5-5
  linkDown trap, B-7
EIA-232C COM Port connector, C-3
ending a session, 2-3
entering system information, 3-7
Enterprise Specific Traps, 3-28, B-9
equipment list, E-1
Escape key, 2-6
ESF Line statistics, 5-19
Ethernet
  Initial Route Destination, 3-28
  Link Down, 5-12
  performance statistics, 5-22
Ethernet port, 3-20
  connector pin assignments, C-7
  default gateway address, 3-31
  MAC address, 5-2
  options, 3-30
even parity, 3-32
Excessive Error Rate
  linkDown trap, B-7
  Threshold, 3-12
External
  Device
    controlling access, 4-4
  Modem
    (Com Port) options, 3-36
    Commands, 3-36
  Transmit Clock, 3-13

F

faceplate, 5-3
field is blank/empty, 2-9
file transfer protocol, 3-24, 5-23
FTP, 5-23
  file transfers, 5-23
  initiating a session, 5-23
  limiting access, 4-4, 4-6
  Login Required, 3-24
  Session, 3-24, 4-6
function keys, 2-5, 2-7

G

Gateway Address, 5-15
  Default, 3-31
General
  LEDs, 5-4
  options, 3-9
  SNMP management options, 3-21
  Traps, 3-28
glossary, vi

H

hardware revision
  NAM, 5-2
Health and Status messages, 5-12
Hop, 5-15

I

ICMP (Internet Control Management Protocol), 5-16
Identity
    displaying, 5-2
Ignore Control Leads, 3-33
Inactivity Timeout, 3-23, 3-34
Initial Route Destination, 3-28
interface
    user, 2-1
Interface Status
    Ethernet port, 3-30
Internal
    Transmit Clock, 3-13
Invert Transmit Clock, 3-13
IP
    default destination, 3-20
    node information, 3-19
    Ping test, 6-18
    Routing Table, 1-1, 5-15
    NMS Validation, 3-25
IP Address, 3-34
    Ethernet port, 3-30
    Gateway, 5-15
    limiting SNMP access, 4-9
    NMS number, 3-25, 3-27
    Node, 3-19

K

keys
    keyboard, 2-6
    screen function, 2-5, 2-7

L

Lamp Test, 5-13, 6-19
last reset, 5-11
LEDs, 6-8
    and control leads
        displaying, 5-3
    descriptions, 5-4
    network interface, 5-5
limiting
    asynchronous terminal access, 4-2
    FTP access, 4-6
    SNMP access, 4-7
        through IP addresses, 4-9
    Telnet access, 4-5
Line
    Build Out (LBO), 3-10
    Coding Format, 3-10
    Framing Format, 3-10
    Loopback, 6-13
Link
    Traps, 3-28
    Traps Interfaces, 3-29
linkUp and linkDown
    events, 3-28
    traps, B-6
LLB, 6-13, 6-15
local
    external DTE loopback, 3-14
locked out, 4-3, 4-10, 6-4
logging in, 2-2
logging out, 2-3
Login, 4-1
    creating, 4-10
    ID, 4-10
    modifying and deleting, 4-11
    Required, 3-22, 3-33, 4-3, 4-5–4-6
Loopback
    DTE, 6-17
    Line, 6-13
    Payload, 6-14
    Port (DTE) Initiated, 3-14
    Remote, 6-15
loopback
    network-initiated, 3-15
Loss of Frame (LOF) LED, 5-5
Loss of Signal (LOS)
    at Network, 5-12, 6-6
    LED, 5-4–5-5
    linkDown trap, B-7

M

MAC address, 5-2
Main Menu screen, 2-4
making input selections, 2-9
Management
    and Communication options, 3-19
    General SNMP
        options, 3-21
    SNMP, 3-21
menu
    branches, 2-4
    Configuration, 3-2
    hierarchy, A-1
    main, 2-4
    path, 2-5
    selecting from, 2-8
Menus, A-1

messages
Device, 5-6
Health and Status, 5-12
Self-Test Results, 5-11
system, 2-5
System and Test Status, 5-11
Test Status, 5-13
MIB
access, 4-8
downloading, B-2
support, B-2
Mode
Test, 5-4
model number, 2-5
modifying a login, 4-11
Monitor
DTR, 3-14
RTS, 3-14
monitoring
DSU/CSU, 5-10
LEDs and control leads, 5-3

N

Name
1 or 2 Access, 4-8
Access, 3-21–3-22
Community, 3-21
navigating the screens, 2-6
Net Link
Port Use, 3-32
Network
assigning data port to time slots, 3-17
cable pin assignments, C-2
Com Link Down, 5-12, 6-6
configuring the interface, 3-10
Initiated LLB, 3-11
Initiated PLB, 3-11
interface
LEDS, 5-5
options, 3-10
time slot assignments, 5-14
network
alarm and event defaults, B-10
Network-Initiated Data Channel Loopback, 3-15
NMS
IP Address, 3-25, 3-27, 4-9
IP Validation, 3-25, 4-9
SNMP security options, 3-25
Node
IP Address, 3-19
IP configuration options, 3-19
Subnet Mask, 3-19
Number of
Managers, 3-25, 4-9
Trap Managers, 3-27

O

odd parity, 3-32
OK LED, 5-4
operation, 2-1
organization of this document, v
Out of Frame (OOF), 5-4
LED, 5-4–5-5
linkDown trap, B-7

P

Parity, 3-32
Password, 4-10
pattern tests, 6-16
Payload Loopback, 6-14
performance statistics, 5-17
clearing, 5-18
physical
data port options, 3-13
network interface options, 3-10
tests, 6-12
pin assignments
COM port, C-3
Ethernet port, C-7
Port-1 V.35 connector, C-6
T1 cable, C-2
T1 line interface cable, C-2
Ping test, 6-18
PLB, 6-14
Port
(DTE) Initiated Loopbacks, 3-14
Access Level, 3-33, 4-3
assigning port to network time slots, 3-17
assignment
clearing, 3-18
communication options, 3-32
connector pin assignments, C-6
Ethernet
connector pin assignments, C-7
interface status, 3-30
LED, 5-5
Use, 3-32
Primary Clock
Failed, 5-13, 6-6
Source, 3-9
problem indicators, 6-2
product-related documents, vi
Proprietary RIP, 3-28

Protocol
Routing Information (RIP), 3-35
Simple Network Management (SNMP), 3-21

R

rear panel, C-1
remote loopbacks, 6-15
reset
last time, 5-11
resetting
statistics, 5-18
the unit, 6-3
unit default configuration options, 6-4
restoring communication with a misconfigured unit, 6-4
revision
software and hardware, 5-2
RFC 1213 and 1573, B-2
RFC 1659, B-2
RIP, 3-35, 5-16
proprietary, 3-28
RJ45 Ethernet Port connector, C-7
RJ48C network cable, C-2
Routing
Information Protocol (RIP), 3-35
IP table, 5-15

S

saving configuration options, 3-6
screen
area, 2-5
function keys area, 2-5
how to navigate, 2-6
scrolling through valid selections, 2-9
security, 2-1–2-2, 3-5, 4-1
SNMP NMS options, 3-25
selecting
a field, 2-9
from a menu, 2-8
Self-Test Results messages, 5-11
Send
and monitor test pattern, 6-16
Pattern, 6-12
serial number
NAM, 5-2
Service and Warranty, A
Session
Access Level, 3-23, 4-5
ending, 2-3
starting, 2-2
setting
Date & Time (system clock), 3-7
date and time, 3-7
setting up
auto-configuration, 3-8
SNMP trap managers, 3-25
so router can receive RIP, 3-7
SIG LED, 5-5
SNMP
assigning community names/access levels, 4-8
limiting access, 4-7, 4-9
Management, 3-21, 4-7
NMS security options, 3-25
Number of Managers, 3-25
setting up Trap Managers, 3-25
Traps, 3-27
downloading, B-2
standards, B-4
software
changing, 5-26
downloading, 5-23
NAM revision, 5-2
Standard_out RIP, 3-35
standards compliance for SNMP Traps, B-4
starting
a session, 2-2
a test, 6-10
statistics, 5-17
selecting performance intervals for display, 5-19
Status
Health and, 5-12
information, 5-10
LED, 5-4
menu/branch, 2-4
test messages, 5-13
time slot assignment, 5-14
Stop Bits, 3-33
stopping a test, 6-10
Subnet Mask, 3-30, 3-34
Node, 3-19
suggestions
user documentation, A
switching
between screen areas, 2-8
to new software, 5-26
System
and test status messages, 5-11
configuring options, 3-9
displaying information, 5-2
entering information, 3-7
General options, 3-9
last reset, 5-11
messages, 2-5, 5-6
Name, Contact, and Location, 5-2
setting the clock (data & time), 3-7

T

T1
- Canadian line interface cable, C-2
- Canadian network cable, C-2
- network interface and cable, C-2
- network interface options, 3-10

tab key, 2-6
TCP, 5-23
Telnet
- limiting access, 4-4–4-5
- Session, 4-5
  - user interface options, 3-22

Terminal
- Port Use, 3-32

Test
- menu/branch, 2-4
- Mode, 5-4
- Status messages, 5-13

Tests, 1-1
- aborting, 6-11
- DTE Loopback, 6-17
- Duration, 3-9
- IP Ping, 6-18
- Lamp, 6-19
- Line Loopback, 6-13
- pattern, 6-16
- Payload Loopback, 6-14
- physical, 6-12
- Remote Line Loopback, 6-15
- starting or stopping, 6-10
- Timeout, 3-9, 6-10

time
- setting, 3-7
- slot assignment
  - network, 5-14
  - status, 5-14
  - synchronous data port-network, 3-17

time slots, 3-16
Timeout
- Inactivity, 3-23, 3-34
- Test, 6-10

trademarks, A
Training, A
transfering data, 5-26
Transmit Clock
- Invert, 3-13
- Source, 3-13

Trap
- Event Log, 5-23
- Number of Managers, 3-27

Traps
- authentificationFailure, B-5
- Enterprise Specific, 3-28, B-9
- General, 3-28
- Link, 3-28
- Link Interfaces, 3-29
- linkUp and linkDown, B-6
- RMON Specific, B-10
- SNMP and dial-out options, 3-27
- standards, B-4
- warmStart, B-5

troubleshooting, 6-1
- device problems, 6-8
- tables, 6-8

TST LED, 5-4
TTL, 5-16
Type
- Access, 3-26

U

upgrading system software, 5-25
uploading data, 5-26
user interface, 2-1
- cannot be accessed, 6-8
- external modem (Com port) options, 3-36
- resetting/restoring access, 6-4
- Telnet session, 3-22

V

V.35
- connector, C-6
- straight-through cable, C-6

V.54 Loopback, 5-13
variable-bindings, B-7

W

warmStart
- events, General Traps, 3-28
- trap, B-5

warranty, A
Web site
- access to Paradyne documentation, vi
- glossary, vi

Y

Yellow Alarm, B-7
- Signal, 5-4–5-5