



**HOTWIRE™ 8786**  
**M/HDSL TERMINATION UNIT**  
**WITH G.703 INTERFACE**  
**USER'S GUIDE**

Document No. 8786-A2-GB20-00

December 1998

---

**Copyright © 1998 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, and Service 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:

- **Via the Internet:** Visit the Paradyne World Wide Web site at <http://www.paradyne.com>
- **Via Telephone:** Call our automated call system to receive current information via 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

## **Trademarks**

All products and services mentioned herein are the trademarks, service marks, registered trademarks or registered service marks of their respective owners.

## **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@eng.paradyne.com](mailto:userdoc@eng.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.



Printed on recycled paper

## Important Safety Instructions

1. Read and follow all warning notices and instructions marked on the product or included in the manual.
2. Slots and openings in the cabinet are provided for ventilation. To ensure reliable operation of the product and to protect it from overheating, these slots and openings must not be blocked or covered.
3. Do not allow anything to rest on the power cord and do not locate the product where persons will walk on the power cord.
4. Do not attempt to install or service this product yourself, as opening or removing covers may expose you to dangerous high voltage points or other risks. Refer all installation and servicing to qualified service personnel.
5. General purpose cables are provided with this product. Special cables, which may be required by the regulatory inspection authority for the installation site, are the responsibility of the customer.
6. When installed in the final configuration, the product must comply with the applicable Safety Standards and regulatory requirements of the country in which it is installed. If necessary, consult with the appropriate regulatory agencies and inspection authorities to ensure compliance.
7. A rare phenomenon can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate buildings are **interconnected**, the voltage potential may cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and, if necessary, implement corrective action prior to interconnecting the products.
8. In addition, if the equipment is to be used with telecommunications circuits, take the following precautions:
  - Never install telephone wiring during a lightning storm.
  - Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
  - Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
  - Use caution when installing or modifying telephone lines.
  - Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
  - Do not use the telephone to report a gas leak in the vicinity of the leak.

## EMI Warnings

### **WARNING:**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The authority to operate this equipment is conditioned by the requirements that no modifications will be made to the equipment unless the changes or modifications are expressly approved by Paradyne Corporation.

### **WARNING:**

To Users of Digital Apparatus in Canada:

This Class A digital apparatus meets all requirements of the Canadian interference-causing equipment regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du règlement sur le matériel brouilleur du Canada.

---

# Contents

---

## About This Guide

- Document Purpose and Intended Audience ..... v
- Document Summary ..... v
- Product-Related Documents ..... vi

## 1 About the Hotwire 8786 Termination Unit

- M/HDSL Overview ..... 1-1
- Hotwire 8786 Termination Unit Features ..... 1-2
- Network Configuration ..... 1-3
- SNMP Management Capabilities ..... 1-4
  - Management Information Base (MIB) Support ..... 1-4
  - SNMP Trap Support ..... 1-4

## 2 Using the Asynchronous Terminal Interface

- User Interface Access ..... 2-1
- Management Serial Port Settings ..... 2-1
- Logging In to the Hotwire DSLAM ..... 2-2
- Selecting the 8786 Card from the DSLAM ..... 2-3
- Initiating an ATI Session ..... 2-4
- Screen Work Areas ..... 2-7
- Navigating the Screens ..... 2-8
  - Keyboard Keys ..... 2-8
  - Screen Function Keys ..... 2-9
  - Switching Between Screen Work Areas ..... 2-10
- Ending an ATI Session ..... 2-11
- Exiting From the DSLAM Session ..... 2-11

### 3 Initial Startup and Configuration

- Overview ..... 3-1
- Entering Identity Information ..... 3-2
- Configuring the 8786 Termination Unit ..... 3-3
  - Configuration Options ..... 3-3
- Accessing and Displaying Configuration Options ..... 3-4
- Configuration Edit/Display ..... 3-5
- Configuring AutoRate ..... 3-6
- Configuration Loader ..... 3-8
- Saving Configuration Options ..... 3-10
- Restoring Access to the User Interface ..... 3-11
- Download Code ..... 3-11

### 4 Monitoring the Unit

- What to Monitor ..... 4-1
- Viewing System and Test Status ..... 4-2
  - Health and Status ..... 4-3
  - Self-Test Results ..... 4-5
  - Test Status ..... 4-6
- Viewing Network Error Statistics ..... 4-7
- Viewing Network Performance Statistics ..... 4-8
- Viewing G.703 Performance Statistics ..... 4-10
- Viewing 8786 Termination Unit LEDs ..... 4-12
- Model 8786 Termination Unit LEDs ..... 4-13

### 5 Testing

- Accessing the Test Menu ..... 5-1
- Running Network Tests ..... 5-2
  - Line Loopback ..... 5-3
  - Repeater Loopback ..... 5-4
  - DTE Loopback ..... 5-5
  - Send Remote Line Loopback ..... 5-6
  - Send and Monitor 511 ..... 5-7
- Device Tests ..... 5-8
  - Lamp Test ..... 5-8
- Ending an Active Test ..... 5-9

## 6 Messages and Troubleshooting

■ Overview .....	6-1
■ Configuring SNMP Traps .....	6-2
■ Device Messages .....	6-3
■ Troubleshooting .....	6-5

## 7 Security

■ Overview .....	7-1
■ ATI Access Levels .....	7-1
■ Creating a Login .....	7-2
■ Deleting a Login .....	7-4
■ Controlling SNMP Access .....	7-4
Assigning SNMP Community Names and Access Types .....	7-4
Limiting SNMP Access through the IP Addresses of the Managers .	7-5

## 8 IP Addressing

■ Selecting an IP Addressing Scheme .....	8-1
■ IP Addressing Example .....	8-2

## A Configuration Option Tables

■ Overview .....	A-1
■ Network Interface Options Menu .....	A-2
■ G.703 Interface Options .....	A-4
■ Copy Port Options .....	A-6
■ System Options .....	A-7
■ Management and Communication Options Menu .....	A-8
Telnet Session Options .....	A-8
SNMP Traps Options .....	A-10
General SNMP Management Options .....	A-13
SNMP NMS Security Options .....	A-15

## B Standards Compliance for SNMP Traps

■ SNMP Traps .....	B-1
warmStart .....	B-1
authenticationFailure .....	B-1
linkUp and linkDown .....	B-2
■ Enterprise-Specific Traps .....	B-3

## **C Connector Pin Assignments**

- Overview ..... C-1
- Hotwire 8600 DSLAM Telco 50-pin Connector Pinouts for DSL Loops .. C-2
- Hotwire 8800 DSLAM Telco 50-pin Connector Pinouts for DSL Loops .. C-3
- Hotwire 8786 Front Panel 50-pin DTE Connector Pinouts ..... C-4

## **D Technical Specifications**

### **Glossary**

### **Index**

---

# About This Guide

---

## Document Purpose and Intended Audience

This guide contains information needed to set up, configure, and operate the 2-port Hotwire 8786 Multirate High-bit-rate Digital Subscriber Line (M/HDSL) Termination Unit and is intended for installers and operators.

## Document Summary

Section	Description
Chapter 1	<i>About the Hotwire 8786 Termination Unit.</i> Describes the Model 8786 Termination Unit's features and capabilities.
Chapter 2	<i>Using the Asynchronous Terminal Interface.</i> Provides instructions for accessing the user interface and navigating through the screens.
Chapter 3	<i>Initial Startup and Configuration.</i> Provides procedures for setting up the user interface, configuration steps, and call setup.
Chapter 4	<i>Monitoring the 8786 Termination Unit.</i> Describes using the LEDs, status, and network statistics to monitor the unit.
Chapter 5	<i>Testing.</i> Provides information about available tests and test setup.
Chapter 6	<i>Messages and Troubleshooting.</i> Provides information on SNMP traps, device messages, and troubleshooting.
Chapter 7	<i>Security.</i> Presents procedures for creating a login, setting the effective access levels, and controlling SNMP access.
Chapter 8	<i>IP Addressing.</i> Provides information and examples regarding IP addresses.

<b>Section</b>	<b>Description</b>
Appendix A	<i>Configuration Option Tables</i> . Contains all configuration options, default settings, and possible settings.
Appendix B	<i>Standards Compliance for SNMP Traps</i> . Contains SNMP trap compliance information.
Appendix C	<i>Cables and Pin Assignments</i> . Contains connector and interface information.
Appendix D	<i>Technical Specifications</i> . Contains physical and regulatory specifications, network and port interfaces, power consumption values, and accessory part numbers.
Glossary	Defines acronyms and terms used in this document.
Index	Lists key terms, acronyms, concepts, and sections in alphabetical order.

## Product-Related Documents

<b>Document Number</b>	<b>Document Title</b>
7985-A2-GB20	<i>Hotwire Model 7985 M/HDSL Standalone Termination Unit User's Guide</i>
7986-A2-GB20	<i>Hotwire Model 7986 M/HDSL Standalone Termination Unit, with G.703 Interface, User's Guide</i>
8000-A2-GB29	<i>Hotwire Management Communications Controller (MCC) Card User's Guide</i>
8600-A2-GN20	<i>Hotwire 8600 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide</i>
8786-A2-GZ40	<i>Hotwire 8786 M/HDSL Termination Unit, with G.703 Interface, Installation Instructions</i>
8800-A2-GN21	<i>Hotwire 8800 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide</i>

Contact your sales or service representative to order additional product documentation.

Most Paradyne documents are also available on the World Wide Web at:

<http://www.paradyne.com>

Select *Service & Support* → *Technical Manuals*

---

# About the Hotwire 8786 Termination Unit

# 1

---

## M/HDSL Overview

Hotwire™ Multirate High-bit-rate Digital Subscriber Line (M/HDSL) products maximize customer service areas by varying the DSL line rate. This ensures symmetric DSL connectivity over a wide range of telephone line distances and transmission line qualities.

Hotwire products can transport at full (2.048 Mbps) or fractional payload rates over a 4-wire, full-duplex circuit over varying distances based on the conditions of the 4-wire loop. Examples include support for router, multiplexer and PBX connections on 24 gauge (.5 mm) cable up to 21,000 feet (6.4 km).

Hotwire M/HDSL is equipped with an automatic configuration capability that reduces the M/HDSL installation process to a simple plug and play mode. Simply connecting the units to the line automatically configures the customer for the maximum data rate supported by the local loop. M/HDSL units can also be configured at fixed line speeds to achieve maximum distances.

## Hotwire 8786 Termination Unit Features

The 2-port Hotwire 8786 M/HDSL Termination Unit is a circuit board mounted in a Hotwire 8600 or 8800 Digital Subscriber Line Access Multiplexer (DSLAM) and used to transport signals at high speeds over a twisted-pair connection.

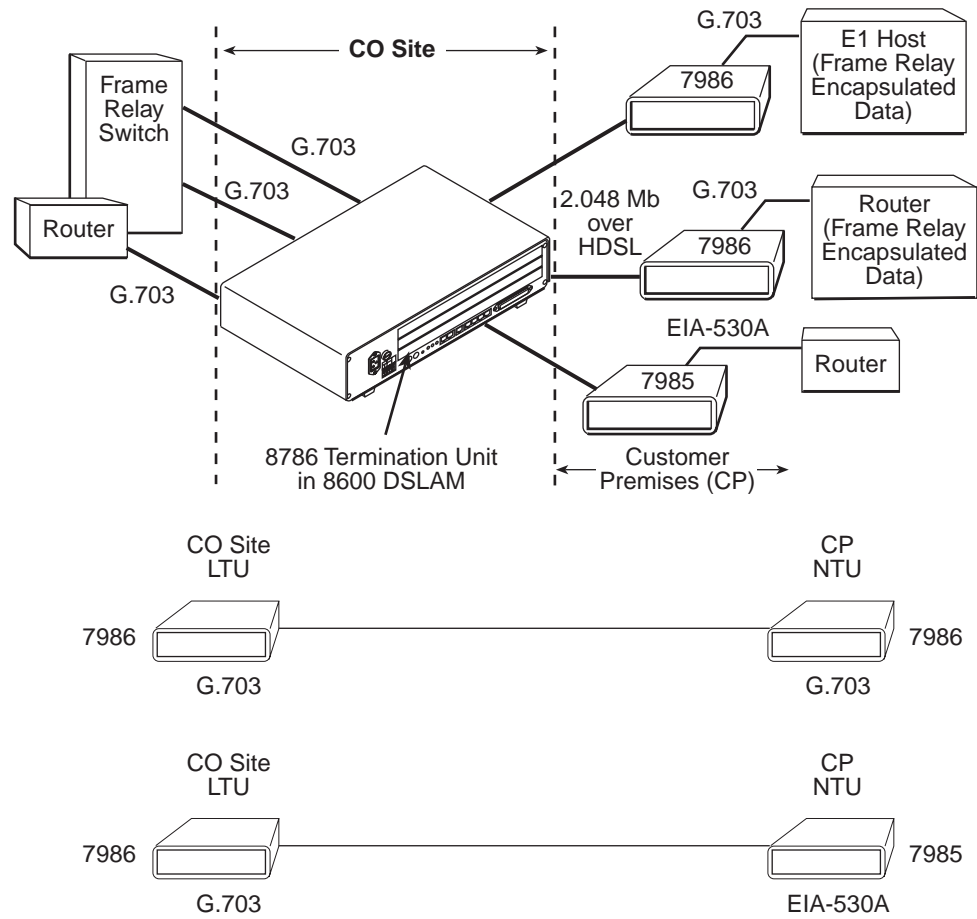
The 8786 Termination Unit offers these standard features:

- **AutoRate Capability.** Provides automatic configuration of line speed and data rate upon connection.
- **Embedded Operations Channel (EOC).** Provides remote management via SNMP or Telnet session capability over the HDSL network.
- **Asynchronous Terminal Interface (ATI).** Provides a menu-driven VE100-compatible terminal interface for configuring and managing the 8786 Termination Unit locally or remotely by Telnet session.
- **Local Management.** Provides local management using the Management Communications Card (MCC) with a:
  - Terminal or PC via the Management Serial port of the DSLAM
  - Network Management System (NMS) via the Management MCC port of the DSLAM
  - NMS connection through the 10BaseT port
- **Remote Management.** Provides remote management:
  - Out-of-band, using an external modem through the Management Serial port of the DSLAM
  - Using SNMP or Telnet through the 10BaseT port or the Internal Management Channel (IMC)
  - Telnet over the EOC
- **Alarm Indication.** Activates front panel LEDs.
- **Diagnostics.** Provides the capability to diagnose device and network problems and perform tests, including digital loopbacks, pattern tests, and self-test.
- **Device and Test Monitoring.** Provides the capability of tracking and evaluating the unit's operation, including health and status, and error-rate monitoring.

## Network Configuration

Figure 1-1 shows an E1 network application using an 8786 M/HDSL Termination Unit for access concentration in a central office (CO). A frame relay switch and a router are connected, through the termination unit, to partner units supporting an E1 host or router, and frame relay encapsulated or unframed data.

This figure also shows a central office-to-standalone configuration using a Hotwire 7985 M/HDSL standalone unit with an EIA-530A interface.



98-16137

Figure 1-1. Sample Configuration

## SNMP Management Capabilities

The termination unit supports SNMP Version 1, and can be managed by any industry-standard SNMP manager and accessed using SNMP by external SNMP managers.

### Management Information Base (MIB) Support

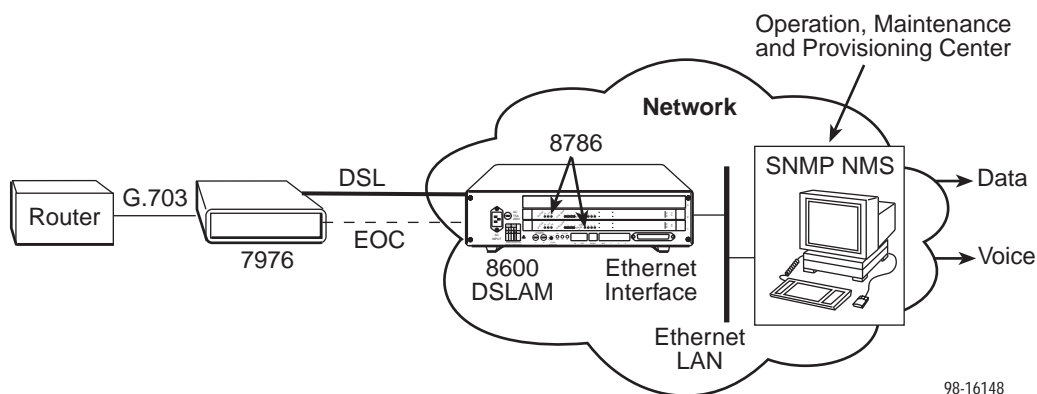
For a detailed description of supported MIBs, visit Paradyne's web site at <http://www.paradyne.com>. The following MIBs are supported:

- **MIB II (RFC 1213 and RFC 1573)** – Defines the general objects for use with a network management protocol in TCP/IP internets and provides general information about the unit. MIB II is backward-compatible with MIB I.
- **DS1/E1 MIB (RFC 1406)** – Reports the performance status of the DSX-1 interface and supports the features found on the DSX-1 Performance Statistics screen.
- **Enterprise MIB** – Supports configuration, status, statistics, and tests.

### SNMP Trap Support

The 8786 Termination Unit supports traps as defined in RFC 1215. They may include variable-bindings specified in the following MIBs:

- **MIB II (RFC 1573)** – Defines the general objects for use with a network management protocol in TCP/IP internets and provides general information about the 8786 Termination Unit. MIB II is backward-compatible with MIB I.
- **Enterprise MIB** – Supports configuration, status, statistics, and tests.



---

# Using the Asynchronous Terminal Interface

# 2

---

## User Interface Access

You can communicate with the asynchronous terminal interface (ATI) using one of the following methods:

- Direct connection through the Management Serial port of the DSLAM (locally or via an external modem).
- Telnet session using a Network Management System (NMS) connected to a LAN port on the DSLAM.
- Telnet session through the Embedded Operations Channel (EOC).

### NOTE:

Only one ATI session can be active at a time, and another user's session cannot be forced to end. To automatically log out a user due to inactivity, enable the Inactivity Timeout option. To enable the Inactivity Timeout option, refer to Table A-5, [Telnet Session Options](#), in Appendix A, *Configuration Option Tables*.

Security can limit ATI access several ways. To set up security or a login ID, refer to Chapter 7, [Security](#).

## Management Serial Port Settings

Ensure that the device you connect communicates using these settings:

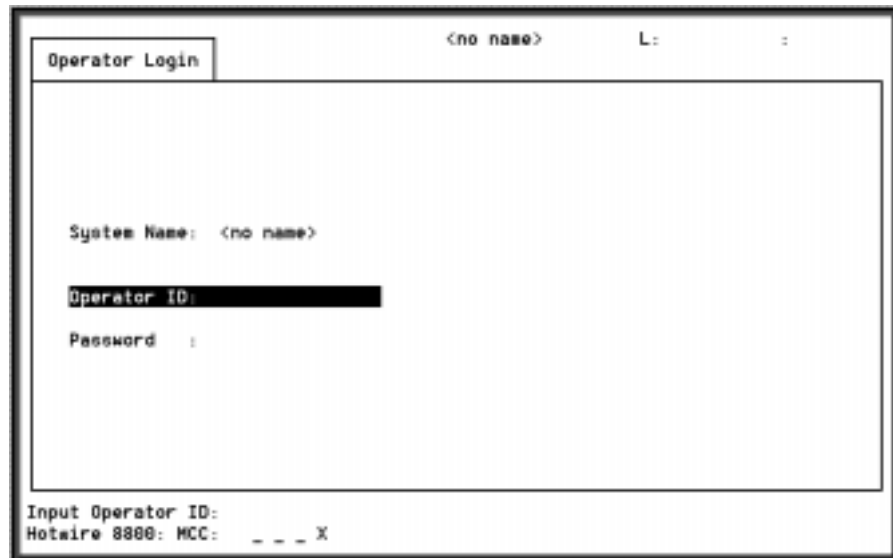
- Data rate set to 9.6 kbps
- Character length set to 8
- Parity set to None
- Stop Bits set to 1
- Flow Control to None

Refer to the Installation Guide for your DSLAM.

## Logging In to the Hotwire DSLAM

You can log in to the Hotwire DSLAM system using either a local VT100-compatible terminal or a remote Telnet connection. The Hotwire DSLAM system accepts only one login session at a time.

At the Operator Login screen, enter your login ID and password.



The screenshot shows a terminal window titled "Operator Login". At the top right, it displays "<no name> L: :". The main area contains the following text:

```
System Name: <no name>
Operator ID: ██████████
Password :
```

At the bottom of the terminal window, the following text is displayed:

```
Input Operator ID:
Hotwire 8880: MCC: _ _ _ X
```

### NOTE:

The login ID and password are case-sensitive; that is, the system recognizes both upper- and lowercase letters. For example, if you enter your user name and password information in upper case letters and your assigned user name and password are in upper- and lowercase letters, the system won't let you log in.

After entering your login ID and password, the system displays the Hotwire Chassis Main Menu.

## Selecting the 8786 Card from the DSLAM

From the Hotwire Chassis Main Menu, select Card Selection to display the cards present in the chassis by type and slot number. The Card Selection screen also displays general and interface status for each card.

```

Card Selection                                     <name>      L:      :
-----
Slot MdlH Stat Eth DSL Lnk WAN Lnk  Slot MdlH Stat Eth DSL Lnk WAN Lnk
M: 8000:  _ _ _ U

4: 8786 :  _ M R   U X

                               14: 8786 :  _ M _   X X
                               15: 8786 :  _ M _   X X

                               Goto Slot(Card) Number:  █

Goto Card (M for MCC or slot# for DSL):
Hotwire 8000: MCC: 8000:  _ _ _ U

```

### ► Procedure

To access the 8786 Termination Unit Main Menu screen:

1. From the Hotwire Chassis Main Menu screen, select Card Selection. The Card Selection screen appears.
2. Verify that the card you want to access appears on the Card Selection screen.
3. At the **Goto Card (M for MCC or slot# for DSL):** prompt, enter the number of the slot, then press Enter. For example, if you want to configure the card in Slot 2, enter **2**.

The 8786 Termination Unit Main Menu appears.

## Initiating an ATI Session

The Main Menu screen is displayed on the screen unless a login ID and password is required or the ATI is already in use.

If the ATI is already in use, you will see a **connection refused** or **connection failed** message (if you are using a Telnet session).

If security is enabled on the 8786 Termination Unit and you used Telnet to access it directly (you did not log in through the MCC), the system prompts you for a login ID and password.

```
Login Slot: 2 Hotwire Model: 8786

                               LOGIN

Login ID: _____
Enter Password: _____

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

After you enter a valid login ID and password, the Main Menu appears. If you enter an invalid login ID and password after three attempts, the Telnet session closes or the terminal connection returns to an idle state. Refer to Chapter 7, *Security*.

```
main Access Level: Administrator Hotwire Model 8786
Slot: 2

                               MAIN MENU

Status
Test
Configuration
Control

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

Screen Area

Screen Function Keys Area

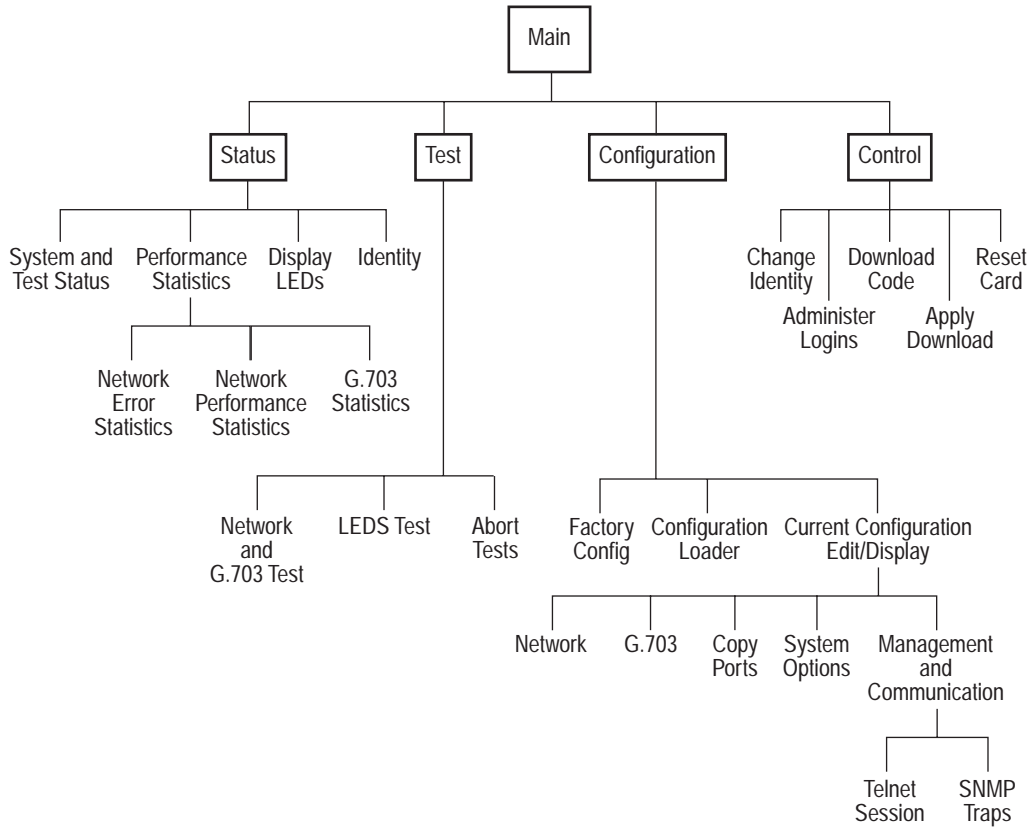
Entry to all of the termination unit's tasks begins at the Main Menu screen. The four branches of the Main Menu are as follows:

Select ...	To ...
Status	View system status, diagnostic test results, statistics, LEDs, and device identity information.
Test	Select, start, stop and cancel tests for the termination unit's interfaces.
Configuration	Display and edit the configuration options.
Control	Change the device identity, administer logins, download new firmware, or initiate a power-up reset of the termination unit.

What appears on the screens depends on your:

- **Current configuration** – How your termination unit is currently configured.
- **Effective security access level** – An access level that is typically set by the system administrator for each interface and each user.
- **Data selection criteria** – What you entered in previous screens.

The following illustration shows the paths to the different ATI screens.



98-16044

## Screen Work Areas

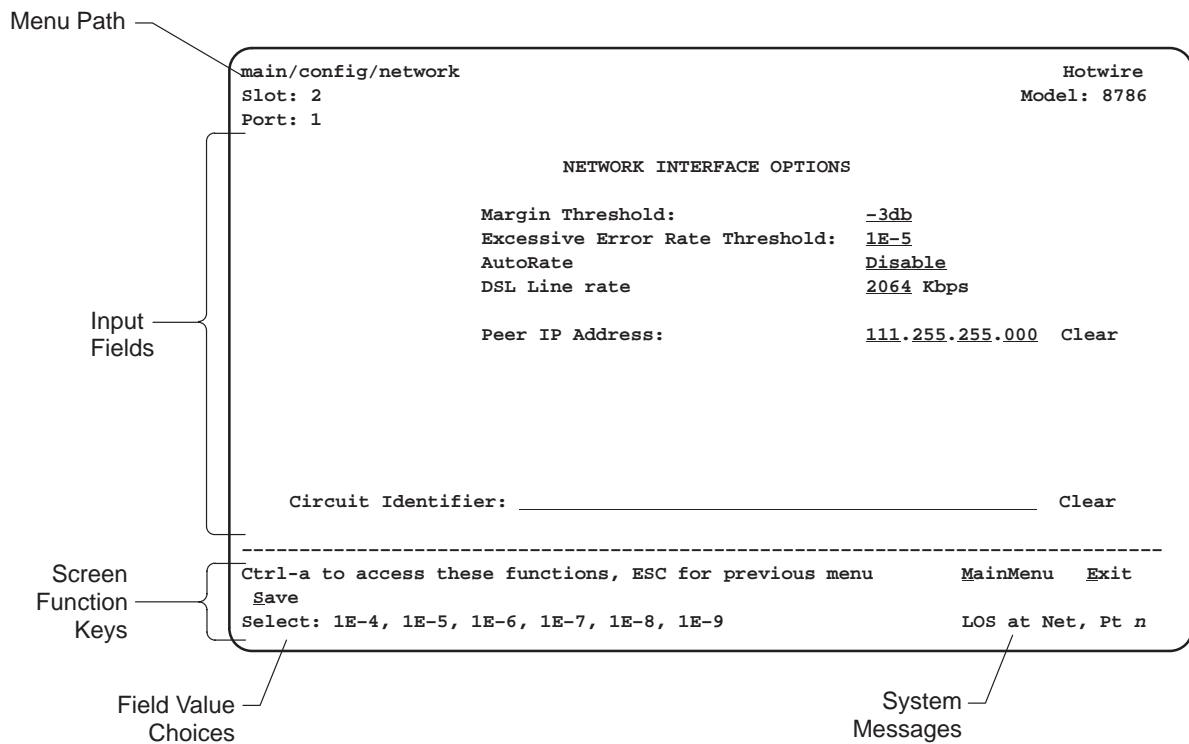
There are two user work areas:

- **Screen area** – This is the area above the dotted line that provides the menu path, menus, and input fields.

The menu path appears as the first line on the screen. In this manual, the menu path is presented as a menu selection sequence with the names of the screens:

*Main Menu → Configuration → Load Configuration From → Network Interface Options*

- **Screen function key area** – This is the area below the dotted line that lists function keys specific to the screen, field value choices, and system messages.



## Navigating the Screens

You can navigate the screens by:

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

### Keyboard Keys

Use the following keyboard keys to navigate within the screen.

Press . . .	To . . .
Ctrl-a	Move cursor between the screen area and the screen function keys area below the dotted line at the bottom of the screen.
Esc	Return to the previous screen.
Tab	Move cursor to the next field on the screen.
Backspace	Move cursor to the previous field on the screen.
Enter	Accept entry or display valid options on the last row of the screen when pressed before entering data or after entering invalid data.
Ctrl-k	Tab backwards (move cursor one field to 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.

#### ► Procedure

To make a menu or field selection:

1. Press the Tab key or the right arrow key to position the cursor on a menu or field selection. Each 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.
3. Continue Steps 1 and 2 until you reach the screen you want.

The current setting or value appears to the right of the field name. You can enter information into a selected field by:

- Typing in the first letter(s) of a field value or command.
- Switching from the screen area to the screen function area below the dotted line and selecting or entering the designated screen function key.

If a field is blank and the Field Values screen area displays valid selections, press the spacebar and the first valid value for the field will appear. Continue pressing the spacebar to scroll through other valid values.

## Screen Function Keys

All screen function keys located below the dotted line operate the same way (upper- or lowercase) throughout the screens.

<b>For the screen function . . .</b>	<b>Select . . .</b>	<b>And press Enter to . . .</b>
Clr <u>F</u> ar	F or f	Clear far-end network statistics and refresh the screen.
Clr <u>N</u> ear	N or n	Clear near-end network statistics and refresh the screen.
Clr <u>S</u> tats	S or s	Clear G.703 statistics and refresh the screen.
De <u>l</u> ete	L or l	Delete data.
<u>E</u> xit	E or e	Terminate the async terminal session.
<u>M</u> ainMenu	M or m	Return to the Main Menu screen.
<u>N</u> ew	N or n	Enter new data.
Pg <u>D</u> n	D or d	Display the next page, or group of entries.
Pg <u>U</u> p	U or u	Display the previous page, or group of entries.
<u>R</u> esetMon	R or r	Reset an active Monitor 511 test counter to zero.
<u>S</u> ave	S or s	Save information.

## Switching Between Screen Work Areas

Select Ctrl-a to switch between the two screen work areas to perform all screen functions.

### ► Procedure

To access the screen function area below the dotted line:

1. Press Ctrl-a to switch from the screen area to the screen function key area below the dotted line.
2. Select either the function's designated (underlined) character or press the Tab key until you reach the desired function key.

*Example:*

To save the current options, type **s** or **S** (Save).

3. Press Enter. The function is performed.
4. To return to the screen area above the dotted line, press Ctrl-a again.

```
main/config/network                               Hotwire
Slot: 2                                           Model: 8786
Port: 1

                                NETWORK INTERFACE OPTIONS

Margin Threshold:                               -3db
Excessive Error Rate Threshold:                 1E-5
AutoRate                                         Disable
DSL Line rate                                   2064

Peer IP Address:                               111.255.255.000 Clear

Circuit Identifier: _____ Clear

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

## Ending an ATI Session

Use the Exit function key from any screen to terminate the session.

### ► Procedure

To end a session with the asynchronous terminal interface:

1. Press Ctrl-a to go to the screen function key area below the dotted line.
2. Save changes if required. A confirmation message appears if you have made but not saved changes to your configuration.
3. Tab to Exit (or type **e** or **E**) and press Enter. If you have accessed the card through the MCC, the Hotwire Chassis Card Selection menu appears.

## Exiting From the DSLAM Session

You can manually log out of the system or, after five minutes of inactivity, the system will automatically log you out if the inactivity time-out option is enabled.

### ► Procedure

To manually exit from the Hotwire DSLAM system:

1. Return to the Hotwire Chassis Main Menu by selecting Exit from either the Hotwire – MCC menu or the Hotwire – DSL menu.  
The Hotwire Card Selection menu appears.
2. From the Hotwire Card Selection menu, type Ctrl-z. The Hotwire Chassis Main Menu appears.
3. From the Hotwire Chassis Main Menu, select Logout.  
The system exits from the current login session on the Hotwire DSLAM.



---

# Initial Startup and Configuration

# 3

---

## Overview

This chapter provides instructions on how to access the system for the first time and perform initial setup procedures. These procedures include:

- Providing initial unit identity information or changing existing identity information.
- Configuring your unit using the Configuration Edit menus.
- Choosing the current or factory default configuration options or downloading configuration options from a TFTP server.
- Modifying current configuration options using the Configuration Edit/Display menu.
- Saving your changes.
- Downloading unit firmware from a TFTP server.

## Entering Identity Information

After accessing your unit for the first time, use the Change Identity screen to determine SNMP administrative system information that will be displayed on the Identity screen of the Status branch. To access the Card Identity screen, follow this menu selection sequence:

*Main Menu → Control → Change Identity*

```

main/control/change_identity                               Hotwire
Slot: 2                                                  Model: 8786

                                IDENTITY

System Name:      111QJ98-001_____                Clear
System Location: Bldg. A412, 2nd Floor, Left cabinet_____ Clear
System Contact:  C. Parker 800-727-2396 pager 888-555-1212 Clear

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

```

The three System entry fields are alphanumeric and provide 128 characters for each field. The System entries appear on the Identity display as shown above. The SNMP System entry fields are:

- **System Name:** The general SNMP system name.
- **System Location:** The physical location of the SNMP-managed device.
- **System Contact:** Identification information, such as contact name, phone number, or mailing address.

Valid entry values are any printable ASCII character. ASCII printable characters include:

- Numeric 0–9
- Upper or lower case A–Z
- Space
- All ASCII symbols except the caret (^)

Select Clear to reset a field to a null value.

### ► Procedure

To enter Change Identity screen information:

1. Position the cursor in the System Name field. Enter a name unique in your network to identify the SNMP managed node (or unit)  
The maximum length of System Name is 128 characters.
2. Position the cursor in the System Location field. Enter the physical location of the unit.  
The maximum length of System Location is 128 characters.
3. Position the cursor in the System Contact field. Enter the name and contact information for the person responsible for the unit.  
The maximum length of System Contact is 128 characters.
4. Press Ctrl-a to switch to the screen function key area below the dotted line.
5. Select Save and press Enter.

## Configuring the 8786 Termination Unit

Configuration option settings determine how the 8786 Termination Unit operates. Use the Configuration branch of the 8786 Termination Unit menu to display or change configuration option settings.

### Configuration Options

The 8786 Termination Unit is shipped with factory settings in the Default Factory Configuration area. You can find default information by:

- Referring to Appendix A, *Configuration Option Tables*.
- Accessing the Configuration branch of the 8786 Termination Unit menu.

The 8786 Termination Unit has two sets of configuration option settings. The Current Configuration matches the Default Factory Configuration until modified and saved by the user.

Configuration Option Area	Configuration Option Set
Current Configuration	The 8786 Termination Unit's active set of configuration options.
Default Factory Configuration	A read-only configuration area containing the factory default configuration options.

If the factory default settings do not support your network's configuration, customize the configuration options for your application.

## Accessing and Displaying Configuration Options

To display the configuration options, you must first load a configuration option set into the edit area.

To load a configuration option set into the configuration edit area, follow this menu selection sequence:

*Main Menu → Configuration (Load Configuration From)*

```

main/configuration                               Hotwire
Slot: 2                                         Model: 8786

                                LOAD CONFIGURATION FROM:

                                Current Configuration
                                Configuration Loader
                                Default Factory Configuration

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

```

Make a selection by placing the cursor at your choice and pressing Enter.

If you select ...	Then ...
Current Configuration	The selected configuration option set is loaded and the Configuration Edit/Display menu screen appears.
Configuration Loader	The Configuration Loader screen is displayed allowing you to upload or download configurations from a TFTP server.
Default Factory Configuration	The selected configuration option set is loaded and the Configuration Edit/Display menu screen appears.

## Configuration Edit/Display

The Configuration Edit/Display screen is displayed when the current, customer, or default configuration is loaded and allows groups of configuration options to be displayed. To access the Configuration Edit/Display screen, follow this menu selection sequence:

*Main Menu → Configuration → Current Configuration*

– or –

*Main Menu → Configuration → Default Factory Configuration*

```

main/config/edit                               Hotwire
Slot: 2                                       Model: 8786

                                CONFIGURATION EDIT/DISPLAY

                                Network
                                G.703
                                Copy Ports
                                System Options
                                Management and Communication

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

Select ...	To Access the ...	To Configure the ...
Network	<a href="#">Network Interface Options</a> , Table A-1	E1 HDSL network interface Ports 1–2.
G.703	<a href="#">G.703 Interface Options</a> Table A-2	G.703 interface.
Copy Ports	<a href="#">Copy Port Options</a> , Table A-3	E1 HDSL network and G.703 interface ports by copying options from port to port.
System Options	<a href="#">System Options</a> , Table A-4	General system options of the unit.
Management and Communication	<ul style="list-style-type: none"> <li>■ <a href="#">Telnet Session Options</a>, Table A-5</li> <li>■ <a href="#">SNMP Traps Options</a>, Table A-6</li> <li>■ <a href="#">General SNMP Management Options</a>, Table A-7</li> <li>■ <a href="#">SNMP NMS Security Options</a>, Table A-8</li> </ul>	Management support of the unit through SNMP and Telnet.

## Configuring AutoRate

The M/HDSL AutoRate function is controlled from the Network Interface Options screen and allows you to enable or disable AutoRate. The AutoRate option is only available if the unit is configured as an LTU. To access the Network Interface screen, follow this menu selection sequence:

### NOTE:

AutoRate is designed to find the best rate possible for your DSL loop conditions. After the DSL loop is up, units should be configured to run in fixed rate.

*Main Menu → Configuration → Network*

```

main/config/network                               Hotwire
Slot 2                                           Model: 8786

                                NETWORK INTERFACE OPTIONS

Margin Threshold:                               -3db
Excessive Error Rate Threshold:                 1E-6
AutoRate                                         Disable
DSL Line Rate                                   528

Peer IP Address:                               111.255.255.000  Clear

Circuit Identifier: _____ Clear

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

```

### ► Procedure

The AutoRate option is defaulted to Disable. To enable AutoRate:

1. Position the cursor in the AutoRate field and press the spacebar.  
The AutoRate field toggles to Enable and the DSL Line Rate field displays.
2. Enter a DSL Line Rate and press Enter.  
Your payload rate is set to a default value of 1984. Use Table 3-1, [Fixed Rate Payload Rates and DSL Line Rates](#), to set your DSL Line Rate and Payload Rate according to whether you are configured for Voice (signaling) or Data.

Table 3-1 provides the maximum payload rates achievable for each DSL line rate and the number of time slots required to achieve that payload rate depending on whether you are using signaling (time slots 0 and 16) or data only (time slot 0).

**Table 3-1. Fixed Rate Payload Rates and DSL Line Rates**

DSL Line Rate (kbps)	Voice Mode (G.703 to G.703)		Data Mode (G.703 to G.703)		Data Mode (G.703 to EIA-530)	
	Maximum Payload Rate (kbps)	Time slots	Maximum Payload Rate (kbps)	Time slots	Maximum Payload Rate (kbps)	Time slots
2064	1920	30	1984	31	1984	31
1552	1408	22	1472	23	1536	24
1040	896	14	960	15	1024	16
784	640	10	704	11	768	12
528	384	6	448	7	512	8
400	256	4	320	5	384	6

## Configuration Loader

The Configuration Loader screen allows you to upload configurations to and download configurations from a TFTP server. To access the Configuration Loader screen, follow this menu selection sequence:

*Main Menu → Configuration → Configuration Loader*

```

main/config/config_loader                               Hotwire
Slot: 2                                                Model: 8786

                                CONFIGURATION LOADER

Image File Name: _____ Clear
TFTP Server IP Address: 000.000.000.000 Clear
TFTP Transfer Direction: Download from Server

Start Transfer: Yes

Packets Sent: 0000000
Packets Received: 0000000
Bytes Sent: 0000000
Bytes Received: 0000000
Transfer Status: Transfer Pending

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

```

### ► Procedure

To upload or download a configuration:

1. Position the cursor in the Image File Name field. Type the name of the file to be downloaded, or the name to be used for the file to be uploaded.

The file name may be a regular path name expression of directory names separated by a forward slash (/) ending with the file name. The total path name length can be up to 128 characters.

*DOS machine:* If the TFTP server is hosted by a DOS machine, then directory and file names must consist of eight or less characters with an optional suffix of up to three characters. The system will automatically upload the configuration file and create directories and file names as needed.

*UNIX machine:* If your server is hosted by a UNIX machine, the configuration file you name must already exist. It will not be created on the UNIX system by the TFTP server. It is critical that you work with your system administrator to plan the naming conventions for directories, filenames, and permissions so that anyone using the system has read and write permissions.

2. Position the cursor in the TFTP Server IP Address field. Enter the TFTP server IP address.

The first three digits of the IP address cannot be 000 or greater than 223.

3. Position the cursor in the TFTP Transfer Direction field. Use the spacebar to select Download from Server or Upload to Server.
4. Position the cursor in the Destination field. Use the spacebar to select a network destination for the TFTP server. Select DSL if the TFTP server destination is the DSL link or IMC if the TFTP destination is the Management port of the MCC.
5. Position the cursor at the Start Transfer field. Use the spacebar to select Yes. Press Enter.

When the data transfer is complete, the Transfer Status field changes to **Completed successfully**.

6. Position the cursor at the Activate new configuration? field and select Yes to activate a new downloaded configuration. Press Enter.

**NOTE:**

The following options are not changed:

- DSL Mode and Telnet Session configuration options
- Peer IP address

You must change these settings with the appropriate configuration menus after the new configuration is activated. See Table A-1, [Network Interface Options](#), Table A-4, [System Options](#), and Table A-5, [Telnet Session Options](#), in Appendix A, *Configuration Option Tables*.

## Saving Configuration Options

When changes are made to the configuration options through the Configuration Edit/Display branch, the changes must be saved to take effect. Use the Save key or Save Configuration screen.

### ► Procedure

To save configuration options changes:

1. Press Ctrl-a to switch to the screen function key area below the dotted line.
2. Select Save and press Enter.

### NOTE:

When Exit is selected before Save, or Save has been selected from any menu in the Configuration/Edit branch, a Save Configuration screen appears requiring a Yes or No response.

```

main/config/saveprompt                               Hotwire
Slot: 2                                             Model: 8786

                SAVE CONFIGURATION

                Save Changes? No_

                WARNING:

                An answer of "yes" will cause the system
                to reset as if it had been powered off and on!

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

```

If the Telnet Session configuration option is changed, a message displays on the Save Configuration screen warning that an answer of Yes will cause the Telnet session to disconnect. Do not answer Yes unless you are prepared to disconnect.

If the HDSL Mode configuration option is changed, the Save Configuration screen bears the warning that an answer of Yes will cause the system to reset. Do not answer Yes unless you are prepared to reset.

If you select ...	Then ...
Yes	The configuration is saved.
No	The Main Menu appears and changes are not saved.

## Restoring Access to the User Interface

Improper configuration of the 8786 Termination Unit could render the user interface inaccessible. If this occurs, access can be restored using the MCC.

### ► Procedure

To reset the DSL Card:

1. Select *Configuration* → *DSL Cards* → *Reset Slot*.
2. Type **DSLnn**, where *nn* is the slot number for the DSL card you wish to reset.
3. Type **Y** at the prompt to confirm.

### NOTE:

When you enter **Y**, all data connectivity is interrupted.

## Download Code

The Download Code screen allows you to download firmware from a TFTP server. To access the Download Code screen, follow this menu selection sequence:

*Main Menu* → *Control* → *Download Code*

```

main/control/download_code                               Hotwire
slot: 2                                                  Model: 8786

                                DOWNLOAD CODE

      Image File Name: _____ Clear
TFTP Server IP Address: 000.000.000.000                Clear
      Destination: DSL

      Start Transfer: Yes

      Packets Sent: 0000000
Packets Received: 0000000
      Bytes Sent: 0000000
      Bytes Received: 0000000
      Transfer Status: Transfer Pending

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

```

► **Procedure**

To download firmware:

1. Position the cursor in the Image File Name field and type the name of the file to be downloaded.

The file name may be a regular path name expression of directory names separated by a forward slash (/) ending with the file name. The total path name length can be up to 128 characters.

2. Position the cursor in the TFTP Server IP Address field and enter the TFTP server IP address.

The first three digits of the IP address cannot be 000 or greater than 223.

3. Position the cursor at the Start Transfer field and use the spacebar to select Yes.

4. Press Enter.

When the data transfer is complete, the Transfer Status field changes to **Completed successfully**.

5. Press the Escape key to return to the Control menu and select Apply Download.

6. Type **Yes** on the Apply Download screen to reset the card and activate the code.

---

# Monitoring the Unit

# 4

---

## What to Monitor

This chapter presents information on how to access and monitor 8786 Termination Unit status and performance statistics on the network. You can monitor 8786 Termination Unit operations by viewing the:

- System and Test Status screen
- Highest priority Health and Status message on the last line of all screens
- Network Error Statistics screen
- Network Performance Statistics screen
- G.703 Performance Statistics screen
- Display LEDs screen or LEDs on the 8786 Termination Unit's front panel

## Viewing System and Test Status

To view System and Test Status information, follow this menu selection sequence:

*Main Menu → Status → System and Test Status*

```
main/status/system                               Hotwire
Slot: 4                                         Model: 8786

                                           SYSTEM AND TEST STATUS                               Page 1 of 1

HEALTH AND STATUS                               SELF-TEST RESULTS                               TEST STATUS
-----
System Operational                               Passed                                           No Test Active

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

The System and Test Status screen has three sections:

- **Health and Status** – Displays messages in priority order (highest to lowest). Refer to Table 4-1, [Health and Status Messages](#).
- **Self-Test Results** – Results of the Diagnostic test run on the device itself. Refer to Table 4-2, [Self-Test Results Messages](#).
- **Test Status** – Currently active tests. Refer to Table 4-3, [Test Status Messages](#).

## Health and Status

The following messages appear in the first column of the System and Test Status screen. The highest priority Health and Status message also appears on all ATI screens on the bottom right.

**Table 4-1. Health and Status Messages (1 of 2)**

Message	What Message Indicates	What To Do
System Operational	There are no problems detected.	
LOS at Net, Pt <i>n</i>	An LOS (Loss Of Signal) condition has been detected on the network interface. No signal is being received on Port <i>n</i> , possibly due to a local network problem.	<ol style="list-style-type: none"> <li>1. Verify that the network cable is securely attached at both ends.</li> <li>2. Verify proper NTU and LTU configuration</li> <li>3. Contact network provider.</li> </ol>
LOF at G.703, Pt <i>n</i>	An LOF (Loss Of Frame) condition has been detected on the G.703 interface.	<ol style="list-style-type: none"> <li>1. Verify that the network cable is securely attached at both ends.</li> <li>2. Verify that the unit's line framing and line coding are compatible.</li> <li>3. Contact network provider.</li> </ol>
AIS at G.703, Pt <i>n</i>	An Alarm Indication Signal (AIS) is being received by the G.703 interface.	<ol style="list-style-type: none"> <li>1. Verify that the unit's line framing and line coding are compatible.</li> <li>2. Verify clock source.</li> <li>3. Contact network provider.</li> </ol>
OOF at Net, Pt <i>n</i>	Three consecutive frame synchronization bits were in error.	Contact network provider.
EER at Net, Pt <i>n</i>	An EER (Excessive Error Rate) condition has been detected on the network interface at Port <i>n</i> . The condition is cleared when the error rate falls below the threshold value currently configured.	<ol style="list-style-type: none"> <li>1. Ignore condition if 511 test active.</li> <li>2. Contact network provider.</li> </ol>
EER at G.703, Pt <i>n</i>	An EER (Excessive Error Rate) condition has been detected on the G.703 interface.	Contact network provider.
RAI (Remote Alarm Indication) at G.703 interface, Pt <i>n</i>	A Remote Alarm Indication signal is being received by the G.703 interface.	Contact network provider.
Net Margin Threshold, Pt <i>n</i>	The signal-to-noise margin has exceeded the configured threshold for Port <i>n</i> .	Contact network provider.

**Table 4-1. Health and Status Messages (2 of 2)**

Message	What Message Indicates	What To Do
Fallback Rate, Pt <i>n</i>	The LTU, set to AutoRate enable, synchronized at a lower rate when the line was restored after an LOS.	Reset AutoRate.  AutoRate is designed to find the best rate possible for your DSL loop conditions. After the DSL loop is up units should be run in fixed rate.
Primary Clock Failed (G.703 Pt <i>n</i> )	A failure has occurred in the primary clock source configured for the G.703 port.	1. Verify that the network cable is securely attached at both ends. 2. Contact network provider.
Device Failed <i>yyyyyyyy</i>	An internal error has been detected by the operating software. <i>yyyyyyyy</i> indicates the 8-digit hexadecimal failure code.	1. Provide the 8-digit failure code shown ( <i>yyyyyyyy</i> ) to your service representative. 2. Reset the 8786 Termination Unit to clear the condition and message.
Download Failed	A firmware download was interrupted.	Repeat the download.
Mismatch Rate, Pt <i>n</i>	The LTU, in fixed rate, is attempting to communicate at a faster rate than the NTU can handle.	1. Verify endpoint is not a 1 Mbps product. 2. Upgrade remote unit to a 2 Mbps or reconfigure the LTU for fixed rate at a lower rate.
NTU TS16 Not Supported	The LTU is configured for TS16 signaling and the NTU is not configured to support TS16 signaling.	1. Verify endpoint is a G.703 product. EIA-530A products do not support signaling. 2. Replace endpoint or reconfigure TS16 to data.

## Self-Test Results

The results of the last power-up or reset self-test appear in the middle column of the System and Test Status screen.

**Table 4-2. Self-Test Results Messages**

Message	What Message Indicates	What To Do
CPU Failed	The CPU failed internal testing.	1. Reset the unit and try again.
DeviceFailed	One or more of the 8786 Termination Unit's integrated circuit chips has failed device-level testing.	2. Call your service representative for assistance.
G.703 Failed, Pt 1	The Unit failed to loop data on the G.703 on Port <i>n</i> .	1. Reset the unit and try again. 2. Call your service representative for assistance.
Net DSL Failed, Pt <i>n</i>	The 8786 Termination Unit failed to loop data on the network DSL circuit of Port <i>n</i> .	1. Reset the unit and try again. 2. Call your service representative for assistance.
Memory Failed	The 8786 Termination Unit failed memory verification.	
Failure xxxxxxx	An internal failure occurred. (xxxxxxx represents an 8-digit hexadecimal failure code for use by service personnel.)	Record the failure code and contact your service representative.
Passed	No errors were detected.	

## Test Status

The Test Status messages in the following table appear in the right column of the System and Test Status screen.

**Table 4-3. Test Status Messages**

Test Status Message	Meaning
No Test Active	No tests are currently running.
LLB Test Active, Pt <i>n</i>	A network Line Loopback test is active on Port <i>n</i> .
RLB Test Active, Pt <i>n</i>	A network Repeater Loopback test is active on Port <i>n</i> .
DLB Test Active, Pt <i>n</i>	A Data Terminal Loopback test is active on Port <i>n</i> .
511 Test Active, Pt <i>n</i>	A 511 Test and Monitor is active on the DSL Port <i>n</i> network interface.
Lamp Test Active	The Lamp Test is active, causing the LEDs on the front panel to light.

For further information on testing, refer to Chapter 5, *Testing*.

## Viewing Network Error Statistics

The 8786 Termination Unit maintains error statistics on the network DSL interface for each port. Port 1 is the default screen selection.

Statistics are maintained for up to 96 15-minute intervals (24 hours).

To view the Network Error Statistics, follow this menu selection sequence:

*Main Menu* → *Status* → *Performance* → *Network Error Statistics*

```

main/status/performance/net_error                               Hotwire
Slot: 4:                                                         Model: 8786
Port: 2                                                         NETWORK ERROR STATISTICS

Current Interval Timer: 2                                       Error Events Counter: 34
-----
      ---ES---          ---SES---          --FEBE--          -Complete-
        Near Far          Near Far          Near Far          Near Far
Current Int: 000 000          000 000          000 000          Yes Yes
Interval 01 000 000          000 000          000 000          Yes Yes
Interval 02 000 000          000 000          000 000          Yes Yes
Interval 03 000 000          000 000          000 000          Yes Yes
Interval 04 000 000          000 000          000 000          Yes Yes
Interval 05 000 000          000 000          000 000          Yes Yes
Interval 06 000 000          000 000          000 000          Yes Yes
Interval 07 000 000          000 000          000 000          Yes Yes

Worst Interval: 24 09          14 08          18 18
Near Tot(valid): 00010          00000          00000
Far Tot(valid): 00010          00000          00000
-----
Ctrl-a to access these functions, ESC for previous menu      MainMenu  Exit
PgUp      PgDn      ClrNear  ClrFar

```

Select a port 1–4 to view error statistics for the port. The default port is 1. Use the virtual function keys to page through the intervals and clear statistics. Select ClrNear or ClrFar to clear the near- and far-end statistics to zero.

Network Error Statistics are collected for all ports for:

- **ES (Errored Seconds):** Seconds during which one or more ESF error events occurred.
- **SES (Severely Errored Seconds):** Seconds during which more than 320 cyclic redundancy check (CRC) error events or at least one Out of Frame (OOF) event occurred.
- **FEBE (Far-End Block Errors):** Errors reported by the remote equipment.
- **Complete:** Whether the interval register contains data for all 900 seconds of the interval.

Use the virtual function keys to page through the intervals and clear statistics.

This Field . . .	Contains . . .
Current Interval Timer	The number of seconds which have elapsed in the current 15-minute interval. Maximum value is 900 seconds (15 minutes). This counter resets every 15 minutes.
Error Events Counter	A running total of CRC errors. Range 0–65535. This counter resets when the near-end data is cleared.
Current Interval	Performance data for the current 15 minutes.
Interval xx	Historical performance data for up to 96 15-minute intervals (24 hours).
Worst Interval	The number of the interval with the worst (highest) performance data for both the near- and far-end statistics. If two or more intervals are equal, the oldest interval is displayed.
Near and Far TOT	A running total of the near- and far-end performance statistics.

## Viewing Network Performance Statistics

Network performance statistics allow you to monitor the current status of the network DSL operations. Performance statistics can assist you in determining the duration of specific conditions and provide a historical context for problem detection and analysis. Statistics are maintained for up to 96 15-minute intervals (24 hours).

To view the Network Performance Statistics, follow this menu selection sequence:

*Main Menu → Status → Performance → Network Performance Statistics*

```

main/status/performance/net_perf
Slot: 4:
Port: 2
Hotwire Model: 8786
NETWORK PERFORMANCE STATISTICS
Current Interval Timer: 002
Payload Rate: 1920 kbps
DSL Line Rate: 2064 kbps
-----
--Mrgn--      --XmtPw--      --RxGn--      -Complete-
Near Far      Near Far      Near Far      Near Far
Current Int: +02 +01      +03 +03      +02 +02      Yes Yes
Interval 01 +02 +03      +03 +03      +02 +02      Yes No
Interval 02 +02 +01      +03 +03      +02 +02      Yes Yes
Interval 03 +02 +01      +03 +03      +02 +02      Yes Yes
Interval 04 +02 +01      +03 +03      +02 +02      Yes Yes
Interval 05 +02 +01      +03 +03      +02 +02      Yes Yes
Interval 06 +02 +01      +03 +03      +02 +02      Yes Yes
Interval 07 +02 +01      +03 +03      +02 +02      Yes Yes
-----
Ctrl-a to access these functions, ESC for previous menu      MainMenu Exit
PgUp      PgDn      ClrNear      ClrFar

```

Select a port to view the performance statistics. The default port is 1. Use the virtual function keys to scroll through the intervals and clear statistics.

This Field . . .	Contains . . .
Current interval timer	The number of seconds which have elapsed in the current 15-minute interval. Maximum value is 900 seconds (15 minutes). This counter resets every 15 minutes.
Payload Rate	The Payload Rate across the DSL interface. Refer to Table 3-1, <i>Fixed Rate Payload Rates and DSL Line Rates</i> , in Chapter 3, <i>Initial Startup and Configuration</i> .
DSL Line Rate	The rate of the DSL line. The line rate can be 400, 528, 784, 1040, 1552, or 2064 kbps.
Current Interval	Performance data for the current 15 minutes.
Interval xx	Historical performance data for up to 96 15-minute intervals (24 hours) where the value of xx is from 01 to 96.

Use the virtual function keys to scroll through the intervals and clear statistics.

Network Performance Statistics are collected for all ports for:

- **MrGn:** Margin, the signal-to-noise ratio (SNR) less an SNR reference value.
- **XmtPw:** The transmit power level.
- **RxGn:** The receiver gain level.
- **Complete:** Whether the interval register contains data for all 900 seconds of the interval.

## Viewing G.703 Performance Statistics

G.703 performance statistics allow you to monitor the current status of the network DSL operations. Performance statistics can assist you in determining the duration of specific conditions and provide a historical context for problem detection and analysis.

Statistics are maintained for up to 96 15-minute intervals (24 hours).

To view the G.703 Performance Statistics, follow this menu selection sequence:

*Main Menu → Status → Performance → G.703 Statistics*

```

main/status/performance/G.703                                     Hotwire
Slot: 4                                                         Model: 8786
Port: 2                                                         G.703 PERFORMANCE STATISTICS

Current Interval Timer: 004                                     Error Events Counter: 012
-----
      ---ES---  --UAS--  --SES--  --BES--  -LOF-  --Status--
Current Int:   000    000    000    000    000    Y
Interval 01:   000    000    000    000    000    NONE
Interval 02:   000    000    000    000    000    NONE
Interval 03:   000    000    000    000    000    NONE
Interval 04:   000    000    000    000    000    NONE
Interval 05:   000    000    000    000    000    NONE
Interval 06:   000    000    000    000    000    NONE
Interval 07:   000    000    000    000    000    NONE

Worst Interval: 12      08      34      18      18
Tot(valid 96): 00010   00000   00000   00000   002
-----
Ctrl-a to access these functions, ESC for previous menu      MainMenu  Exit
PgUp      PgDn      ClrStats

```

Select a port to view the performance statistics. The default port is 1.

G.703 Performance Statistics are collected for all ports for:

- **ES (Errored Seconds):** Seconds during which one or more error events occurred.
- **UAS (Unavailable Seconds):** Seconds during which service is unavailable. UAS is received at the start of 10 consecutive SES and cleared at the start of 10 seconds with no SES.
- **SES (Severely Errored Seconds):** Seconds during which 805 or more cyclic redundancy check (CRC) error events, 16 or more FAS errors, or at least one Out of Frame (OOF) event occurred.

- **BES (Bursty Errored Seconds):** Contains the number of bursty errored seconds for the current interval. A bursty errored second is any second with more than one but less than 805 CRC errors (CRC Mode) or more than one but less than 16 FAS errors (non-CRC mode).
- **LOF (Loss of Frame Seconds):** Contains the number of seconds that contain one or more LOF events.
- **Status:** Contains the contents of the status events register. The status events register maintains a history of specific events that have occurred during an interval. Values include:
  - Y – Remote alarm indication signal received at the G.703 interface
  - L – Loss of signal detected at the G.703 interface
  - E – Excessive error rate threshold exceeded
  - F – Frame synchronization bit error detected
  - V – Line code violation detected
  - None – No significant events have occurred

Use the virtual function keys to page through the intervals and clear statistics.

This Field . . .	Contains . . .
Current Interval Timer	The number of seconds which have elapsed in the current 15-minute interval. Maximum value is 900 seconds (15 minutes). This counter resets every 15 minutes.
Error Events Counter	A running total of CRC errors. Range 0–65535. This counter resets when the statistics are cleared.
Current Interval	Performance data for the current 15 minutes.
Interval xx	Historical performance data for up to 96 15-minute intervals (24 hours).
Worst Interval	The number of the interval with the worst (highest) performance data statistics. If two or more intervals are equal, the oldest interval is displayed.
TOT	A running total of the performance statistics.

## Viewing 8786 Termination Unit LEDs

The 8786 Termination Unit LEDs can be viewed on the Display LEDs Status screen. This ATI status screen is available locally and remotely.

The three groups of LEDs are:

- **General** LEDs display the status of the unit
- **G.703** LEDs provide the status of the G.703 interface
- **DSL Loop** LEDs display the activity on the DSL network

To view the LED status screen, follow this menu selection sequence:

*Main Menu → Status → Display LEDs*

```

main/status/leds                               Hotwire
Slot: 4                                         Model: 8786

                                DISPLAY LEDs

                                GENERAL          G.703          DSL LOOP
-----
                                ALRM:Off      P1:Lnk Up      P1:Lnk Up
                                TEST:On       P2:RAI        P2:Startup
                                                P3:AIS        P3:Lnk Dn
                                                P4:LOF        P4:Lnk Dn

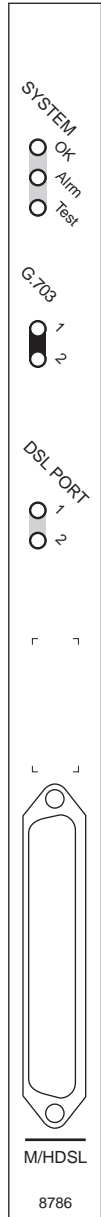
-----
                                ESC for previous menu      MainMenu      Exit

```

The LED status display screen is updated every 5 seconds. For information about the meaning of 8786 Termination Unit LEDs, see *Model 8786 Termination Unit LEDs* on page 4-13.

## Model 8786 Termination Unit LEDs

The following table describes the meaning and states of the LEDs on the 8786 Termination Unit faceplate.



Type	LED	LED is . . .	Indicating . . .
SYSTEM	OK	Green	Normal operation; termination unit functioning normally.
		Off	No power to termination unit, or failure has occurred.
	Alarm	Amber	Device failure, or Power-On Self-Test (POST) failed.
Off		No alarms.	
SYSTEM	Test	Amber	Loopback test or 511 test pattern in progress.
		Amber, flashing	POST in progress.
		Off	No tests currently active.
G.703	1, 2	Green	Recoverable signal present on the G.703 network.
		Amber	Remote Alarm Indication (RAI) present.
		Amber, flashing	An LOF, AIS, or EER condition exists.
		Off	The G.703 LINK is down or disabled.
DSL PORT	1, 2	Green	DSL link is up.
		Amber	DSL training in progress.
		Amber, flashing	OOF condition.
		Off	DSL link is down or disabled.

8786  
98-16136



---

# Testing

# 5

---

## Accessing the Test Menu

From the Test menu, you can run network tests, data port tests, a lamp test for the front panel LEDs, or abort all tests.

To access the Test menu, follow this menu selection sequence:

*Main Menu → Test*

```
main/test                                     Hotwire
slot 4                                       Model: 8786

                                TEST

                                Network & G.703 Tests
                                Device Tests

                                Abort All Tests

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

Select ...	To ...
Network and G.703 Tests	Start and stop tests on the G.703 and network interface.
Device Tests	Start and stop lamp test.
Abort All Tests	To abort all current tests excluding Network-initiated loopback tests. An aborted test may continue to run for a few seconds as the abort command is sent to the remote end and processed.

## Running Network Tests

Network tests require the participation of your network service provider. To access the Network Tests screen, follow this menu selection sequence:

*Main Menu → Test → Network Tests*

```

main/test/network_G703                                     Hotwire
Slot: 4                                                    Model: 8786
Port: 2

                                NETWORK & G.703 TESTS

Test                Command  Status   Results
-----
Local Loopbacks
Network Line Loopback:      Start   Inactive 00:00:00
G.703 Repeater Loopback:    Start   Inactive 00:00:00
G.703 DTE Loopback:         Start   Inactive 00:00:00

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

Network Pattern Tests
Send and Monitor 511        Stop    Active   hh:mm:ss - Errors 99999+
-----
Ctrl-a to access these functions, ESC for previous menu   MainMenu  Exit
ResetMon

```

Use the **Command** column to start or stop a test. When the **Status** column shows that a test is Inactive, Start is displayed; when a test is Active, Stop is displayed. Position the cursor at the desired Start or Stop command and press Enter.

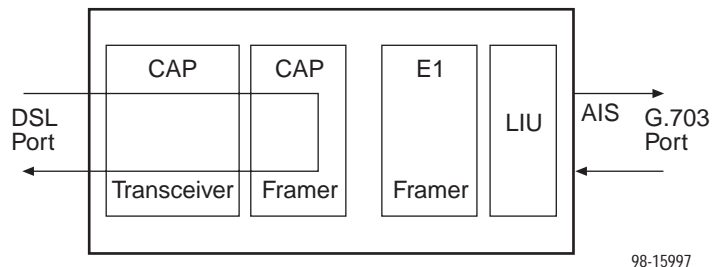
Selecting a Stop command on the Network Tests screen or Abort All Tests from the Test menu will not disrupt a network-initiated loopback.

The **Results** column displays the test duration.

When the Send and Monitor 511 test is active, ResetMon is available to reset the error counter to zero.

## Line Loopback

Line Loopback (LLB) loops the received signal on the network interface back to the network without change.



### ► Procedure

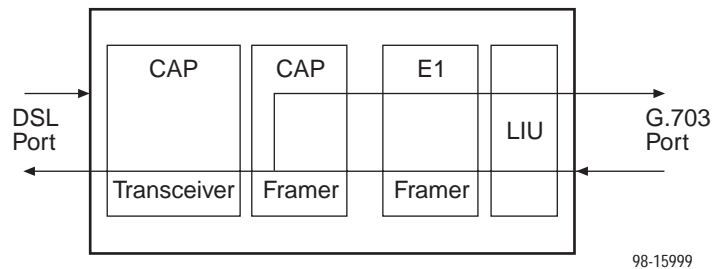
To run a Line Loopback:

1. Position the cursor at the Start command next to Line Loopback on the Network Tests screen.
2. Press Enter.  
The Start command is changed to Stop.
3. To manually stop the test, verify that the cursor is positioned at the Stop command.
4. Press Enter.

Line Loopback cannot be started when a Repeater Loopback, DTE Loopback, or network-initiated Line Loopback or pattern test is in progress.

## Repeater Loopback

Repeater Loopback (RLB) loops the signal being sent from the data port back to the data port and to the network interface.



### ► Procedure

To run a Repeater Loopback:

1. Position the cursor at the Start command next to Repeater Loopback on the Network Tests screen.
2. Press Enter.  
The Start command is changed to Stop.
3. To manually stop the test, verify that the cursor is positioned at the Stop command.
4. Press Enter.

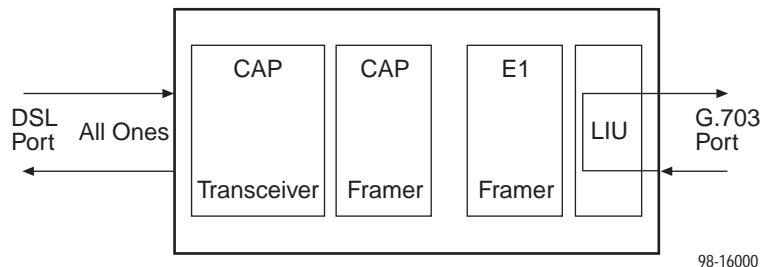
A Repeater Loopback cannot be started when any other loopback or pattern test is in progress.

### **NOTE:**

Activating the Repeater Loopback test causes the EOC to be lost to the remote unit.

## DTE Loopback

DTE Loopback loops the G.703 signal back to itself before the signal is sent to the Framer.



### ► Procedure

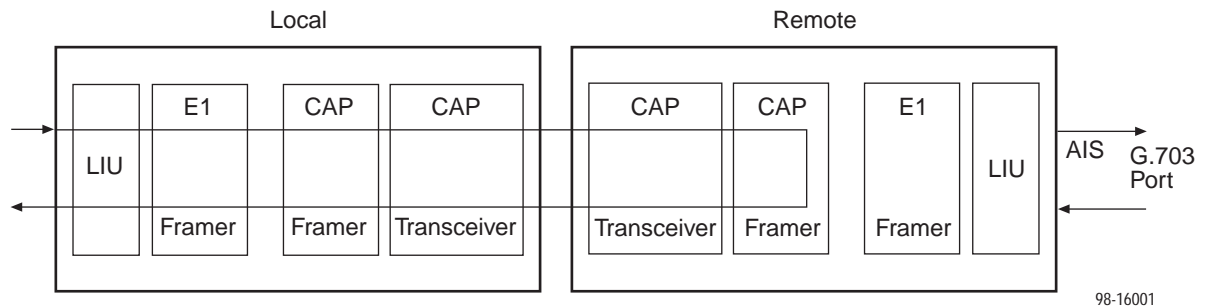
To run a DTE Loopback:

1. Position the cursor at the Start command next to DTE Loopback on the Network Tests screen.
2. Press Enter.  
The Start command is changed to Stop.
3. To manually stop the test, verify that the cursor is positioned at the Stop command.
4. Press Enter.

A DTE Loopback cannot be started when any other loopback test is in progress.

## Send Remote Line Loopback

The local unit initiates this test by sending a line loopback up or down command to the remote unit for 10 seconds. When the remote unit detects the loopback up command, it puts itself in line loopback and lights the front panel test LED. The remote unit remains in loopback until it receives a loopback down command or the remote unit's test timeout value is exceeded. The send line loopback tests both units. External equipment can be used to verify the link.



### ► Procedure

To run a Remote Send Line Loopback:

1. Position the cursor at the Up or Down selection next to Send Line Loopback on the Network Tests screen.
2. Press the spacebar to select either Up or Down.
3. Position the cursor at the Send command next to Up or Down selection.
4. Press Enter.

The local unit stops sending the loopback command automatically after 10 seconds. You cannot stop the Send Remote Line Loopback test manually.

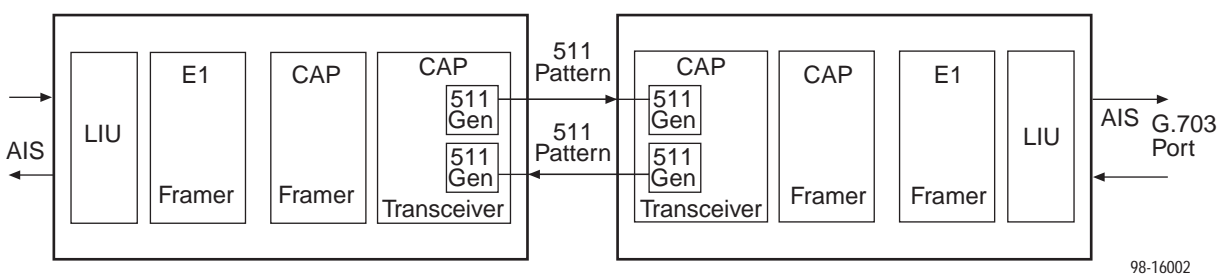
The Send Remote Line Loopback cannot be started when any other loopback or a Send and Monitor 511 test is active on the network interface.

## Send and Monitor 511

The LTU initiates the test by lighting the Test LED then sending a command to the remote unit to send a 511 test pattern. When the remote unit detects the command, it sends a 511 pattern and lights the front panel test LED. Each unit will send and monitor the 511 pattern. The duration and results of the test are displayed on the Network Test screen of the initiating unit.

### NOTE:

The send and monitor test is not a loopback test. Each unit independently sends and monitors a 511 pattern.



### ► Procedure

To run a Send and Monitor 511 test:

1. Position the cursor at the Start command next to Send and Monitor 511 on the Network Tests screen.
2. Press Enter.  
The Start command is changed to Stop.
3. To manually stop the test, verify that the cursor is positioned at the Stop command.
4. Press Enter.

When a Send and Monitor 511 test is active, a count of bit errors is displayed next to the test duration, and the ResetMon virtual function key is available for use. Type r or R or select the ResetMon virtual function key to reset the error count.

## Device Tests

The Device Tests branch is used to access the only card-level test, the Lamp Test. To access the Card Tests screen, follow this menu selection sequence:

*Main Menu → Test → DeviceTests*

```
main/test/device                               Hotwire
Slot: 4                                         Model: 8786

                                DEVIce TESTS

                                Test      Command  Status
-----
                                Lamp Test: Start  Inactive

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

## Lamp Test

The Lamp test determines whether all LEDs are lighting and functioning properly.

### ► Procedure

To test the LEDs:

1. Position the cursor at the Start command next to Lamp Test on the Card Tests screen.
2. Press Enter.  
The Start command is changed to Stop. During the Lamp test, all LEDs blink simultaneously every second. When you stop the Lamp test, the LEDs are restored to their normal condition.
3. To stop the lamp test, position the cursor at the Stop command.
4. Press Enter.

---

## Ending an Active Test

Except for the Remote Send Line Loopback, a test initiated by the user can be ended by the user. Tests can also be terminated automatically by enabling the Test Timeout option from the System Options Menu.

- A Test Timeout option is available to automatically terminate a user-initiated Loopback or Pattern test (as opposed to manually terminating a test) after it has been running a specified period of time. The default is 10 minutes. Refer to Table A-4, [System Options](#).
- On each test screen is a Command column. To stop the test, press Enter when the cursor is on the Stop command.
- Use the Abort All Tests selection from the Test menu to stop all tests running on all interfaces, with the exception of network-initiated loopbacks. **Command Complete** appears when all tests on all interfaces have been terminated.

An aborted test may continue to run for a few seconds as the abort command is sent to the remote end and processed.



---

# Messages and Troubleshooting

# 6

---

## Overview

There are many messages available to assess the status of the device and contribute to problem resolutions. Refer to the following sections:

- *Configuring SNMP Traps*
- *Device Messages*
- *Troubleshooting*

## Configuring SNMP Traps

An SNMP trap can be automatically sent out through the EOC or the Management port to the SNMP manager when the 8786 Termination Unit detects conditions set by the user. These traps enable the SNMP manager to gauge the state of the network. Refer to Appendix B, *Standards Compliance for SNMP Traps*, for details of SNMP traps supported by the 8786 Termination Unit.

To configure the 8786 Termination Unit for SNMP traps, use the SNMP Traps Options screen to:

- Enable SNMP traps.
- Set the number of SNMP managers that receive SNMP traps from the 8786 Termination Unit.
- Enter an IP address and network destination for each SNMP manager specified.
- Select the type of SNMP traps to be sent from the 8786 Termination Unit.

To configure SNMP Traps, follow this menu selection sequence:

*Main Menu → Configuration → Load Configuration From → Management and Communication Options → SNMP Traps Options*

```

main/config/management/trap
Slot: 4
Hotwire
Model: 8786

SNMP TRAPS OPTIONS

SNMP Traps:          Enable          Number of Trap Managers: 5

NMS 1 IP Address: 135.014.040.001 Clear
NMS 2 IP Address: 135.014.003.027 Clear
NMS 3 IP Address: 135.014.001.008 Clear
NMS 4 IP Address: 135.014.002.024 Clear
NMS 5 IP Address: 204.128.146.035 Clear

General Traps:          Both
Enterprise Specific Traps: Disable
Link Traps:             Both
Link Traps Interfaces:  All

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

Refer to Table A-6, *SNMP Traps Options* to configure SNMP traps.

## Device Messages

The Device Messages in Table 6-1, listed in alphabetical order, may appear in the messages area at the bottom of the ATI screens.

**Table 6-1. Device Messages (1 of 2)**

Device Message	What Message Indicates	What To Do
Access level=Operator. Configuration is read-only.	The operator requested that configuration options be loaded, but does not have authority to edit them.	If configuration options are to be edited, use a Login ID that has Administrator authority.
Cannot Save – no Login IDs with Access Administrator	All of the login IDs being saved have an access level below Administrator.	Change the access level of at least one Login ID to Administrator so that configuration changes can be made. (Operator-level users cannot make configuration changes.) Save the Login IDs.
Command Complete	Action requested has successfully completed.	No action needed.
Invalid Character	A nonprintable ASCII character has been entered.	Reenter information using valid characters.
Invalid Password	Login is required and an incorrect password was entered; access is denied.	<ul style="list-style-type: none"> <li>■ Try again.</li> <li>■ Contact your system administrator to verify your password.</li> </ul>
Invalid – Send Pattern Already Active	A pattern test was already in progress when the Start field was selected.	<ul style="list-style-type: none"> <li>■ Allow test to continue.</li> <li>■ Select another test.</li> <li>■ Stop the test.</li> </ul>
Invalid – [Test] Already Active	The described test was already in progress when another selection was made.	<ul style="list-style-type: none"> <li>■ Allow test to continue.</li> <li>■ Select another test.</li> <li>■ Stop the test.</li> </ul>
Invalid Test Combination	A 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.	<ul style="list-style-type: none"> <li>■ Wait until other test ends and message clears.</li> <li>■ Abort all tests from the Test menu screen.</li> <li>■ Stop the test from the same screen the test was started from.</li> </ul>
IP address not in MCC subnet <i>nnn.nnn.nnn.nnn</i>	The IP address specified is not in the same subnet as the MCC.	Enter an IP address that is in the same subnet as the MCC.

**Table 6-1. Device Messages (2 of 2)**

Device Message	What Message Indicates	What To Do
Command Failed		<ul style="list-style-type: none"> <li>■ Try again.</li> <li>■ Contact your system administrator to verify your password.</li> </ul>
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.	<ol style="list-style-type: none"> <li>1. Delete another login/password combination.</li> <li>2. Reenter the new login ID.</li> </ol>
No Security Records to Delete	Delete was selected from the Administer Login screen, and no security records had been defined.	<ul style="list-style-type: none"> <li>■ No action needed.</li> <li>■ Enter a security record.</li> </ul>
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.	<ul style="list-style-type: none"> <li>■ Try again.</li> <li>■ Contact your system administrator to verify your password.</li> </ul>
Please Wait	Command takes longer than 5 seconds.	Wait until message clears.
Test Active	A test is running and no higher priority health and status messages exist.	<ul style="list-style-type: none"> <li>■ Contact service provider if test initiated by the network.</li> <li>■ Wait until the other test ends and message clears.</li> <li>■ Cancel all tests from the Test screen.</li> <li>■ Stop the test from the same screen the test was started from.</li> </ul>
0.0.0.0 is an invalid IP address	An IP address of all zeroes was entered.	Enter a valid, non-zero IP address.

## Troubleshooting

This 8786 Termination Unit is designed to provide you with many years of trouble-free service. If a problem occurs, however, refer to Table 6-2 for possible solutions.

**Table 6-2. Troubleshooting (1 of 2)**

Symptom	Possible Cause	Solutions
Alarm LED is on.	A system failure has occurred.	Refer to Table 4-1, <a href="#">Health and Status Messages</a> in Chapter 4, <i>Monitoring the Unit</i> , for a recommended action.
Cannot access the Unit via the ATI.	The terminal is not set up for the correct rate or data format, or the 8786 Termination Unit is configured so it prevents access.	<ul style="list-style-type: none"> <li>■ Check the cable and connections.</li> <li>■ Ensure that the Unit is configured properly in the DSLAM. Verify its IP address.</li> <li>■ Reset the Unit.</li> </ul>
Device Fail appears on the System and Test Status screen under Self-Test results.	The 8786 Termination Unit detects an internal hardware failure.	<ul style="list-style-type: none"> <li>■ Reset the Unit.</li> <li>■ Contact your service representative.</li> </ul>
No power, or the LEDs are not lit.	The power cord is not securely plugged into the wall receptacle and into the rear panel connection.	Check that the power cord is securely attached at both ends.
	The wall receptacle has no power.	<ul style="list-style-type: none"> <li>■ Check the wall receptacle power by plugging in some equipment that is known to be working.</li> <li>■ Check the circuit breaker.</li> <li>■ Verify that your site is not on an energy management program.</li> </ul>
	Power supply has failed.	Replace power supply.
An LED is not lit.	LED is out.	Run the Lamp test. If the LED in question does not flash with the other LEDs, then contact your service representative.

**Table 6-2. Troubleshooting (2 of 2)**

Symptom	Possible Cause	Solutions
Not receiving data.	<ul style="list-style-type: none"> <li>■ The network or data port cables are not connected (check front panel LEDs for more information).</li> <li>■ A test is being executed on the unit (check the TEST LED on the front panel).</li> <li>■ The G.703 Port is not enabled.</li> <li>■ The far-end device is offline.</li> </ul>	<ul style="list-style-type: none"> <li>■ Check network and data port cables.</li> <li>■ Run Loopback tests. Refer to Chapter 5, <i>Testing</i>.</li> <li>■ Stop the test or wait for the test to end.</li> <li>■ Enable the G.703 Port.</li> <li>■ Make sure the far-end device is on.</li> </ul>
Power-Up Self-Test fails. Only Alarm LED is on after power-up.	The 8786 Termination Unit has detected an internal hardware failure.	<ul style="list-style-type: none"> <li>■ Reset the unit and try again.</li> <li>■ Contact your service representative.</li> </ul>

---

# Security

# 7

---

## Overview

The 8786 Termination Unit provides several methods of security by limiting user access to the ATI through option settings. You can:

- Enable the Telnet Login Required option.
- Limit the access by setting a Session Access Level option of Operator for the Telnet Session.
- Disable the access with the Telnet Session option.

See Table A-5, [Telnet Session Options](#), in Appendix A, *Configuration Option Tables*.

## ATI Access Levels

The 8786 Termination Unit has two access levels: Administrator and Operator. The access level determines what functions are accessible, as follows.

**Table 7-1. Access Levels**

ATI Access to Menu Functions	Administrator	Operator
Status	Read-Only	Read-Only
Test	Full Access	No Access
Configuration	Full Access	Read-Only
Control	Full Access	No Access

The effective access level is the more restrictive of the session access level or the login access level.

Access level is also used to control access via Telnet. If the Telnet Session Access Level is set to Administrator (see Table A-5, [Telnet Session Options](#)), a Login ID with an Operator access level is not permitted access.

## Creating a Login

Logins apply to Telnet access directly to the ATI of the 8786 Termination Unit. The Administer Logins menu option is not presented when you access the unit through the MCC.

Six login ID/password combinations are available. Each Login ID and Password must be unique and include an access level.

### ► Procedure

- To create a login record, follow this menu selection sequence:

*Main Menu → Control → Administer Logins*

```

main/control/admin_logins                               Hotwire
Slot: 4                                                Model: 8786

                                ADMINISTER LOGINS                               Page 1 of 1

Login ID:                newuser
Access Level:            Administrator

                                Are You Sure? Yes

-----
Save  PgUp  PgDn                                ESC for previous menu  MainMenu  Exit
                                         New          Delete
  
```

- Select New and press Enter. The Login Entry screen appears.

```

main/control/admin_logins                               Hotwire
Slot: 4                                                Model: 8786

                                LOGIN ENTRY

Login ID:                newuser
Password:                e34t136
Re-enter Password:      e34t136
Access Level:            Administrator

                                WARNING
                                New logins will not become permanent until saved
                                through the "ADMINISTER LOGINS" screen!

-----
Ctrl-a to access these functions  ESC for previous menu  MainMenu  Exit
Save  PgUp  PgDn                                         New          Delete
  
```

3. Create the login by entering the following fields. Login IDs and passwords are case-sensitive.

<b>On the Login Entry screen, for the . . .</b>	<b>Enter . . .</b>
Login ID	1 to 10 ASCII printable characters (hex21 through 7E). Blanks are not allowed.
Password	1 to 10 ASCII printable characters that can consist of 0–9, a–z, A–Z, # (pound), . (period), – (dash), and / (slash).
Re-enter Password	1 to 10 ASCII printable characters characters that can consist of 0–9, a–z, A–Z, # (pound), . (period), – (dash), and / (slash).
Access Level	Administrator, Operator

**NOTE:**

Assign at least one Administrator-level Login ID. Full access is necessary to make configuration option changes and administer logins.

4. Press Ctrl-a to switch to the screen function key area below the dotted line. Select Save and press Enter.
5. When Save is complete, **Command Complete** appears at the bottom of the screen.
6. If additional logins are required, repeat Steps 3 through 5.
7. When all logins are entered, press Esc to return to the Administer Logins screen.
8. Select Save and press Enter.

## Deleting a Login

### ► Procedure

1. To delete a login record, follow this menu selection sequence:  
*Main Menu → Control → Administer Logins*
2. Select PgUp or PgDn and press Enter to page through login pages/records until you find the one to be deleted.
3. Once the correct record is displayed, select De|lete and press Enter.
4. To complete the delete action, select Save and press Enter.  
When the deletion is complete, **Command Complete** appears at the bottom of the screen. The number of login pages/records reflects one less record, and the record following the deleted record appears.

## Controlling SNMP Access

There are three methods for limiting SNMP access.

- Disable the SNMP management option. Refer to Table A-7, **General SNMP Management Options**.
- Assign SNMP community names and access types.
- Limit SNMP access through validation of the IP address of each allowed SNMP manager.

## Assigning SNMP Community Names and Access Types

The unit can be managed by an SNMP manager supporting SNMP. The community name must be supplied by an external SNMP manager accessing an object in the MIB.

To define SNMP community names, follow this menu selection sequence:

*Main Menu → Configuration → Load Configuration From → Edit →  
SNMP → General SNMP Management*

Refer to Table A-7, **General SNMP Management Options**, to:

- Enable SNMP Management.
- Assign the SNMP community names of the SNMP Managers that are allowed to access the unit's Management Information Base (MIB).
- Specify Read or Read/Write access for each SNMP community name.

## Limiting SNMP Access through the IP Addresses of the Managers

The unit provides an additional level of security through validation of the IP addresses.

The SNMP Management option must be enabled. To control SNMP access with IP addresses, follow this menu selection sequence:

*Main Menu → Configuration → Management → Security Menu*

Refer to Table A-8, **SNMP NMS Security Options**. The SNMP access can be limited by:

- Enabling NMS IP address checking.
- Add each IP address and access level.

### **NOTE:**

Do not change or delete the IP address or access level of the NMS performing the sets or enable IP address checking prior to adding the NMS to the table.



## Selecting an IP Addressing Scheme

The NTU's network interface IP address is assigned through the peer IP address of the LTU's Network Interface menu. The NTU obtains the LTU's IP address and subnet mask when the PPP link is established over the EOC. The LTU IP address and subnet mask are configured from the Communication Protocol Options menu.

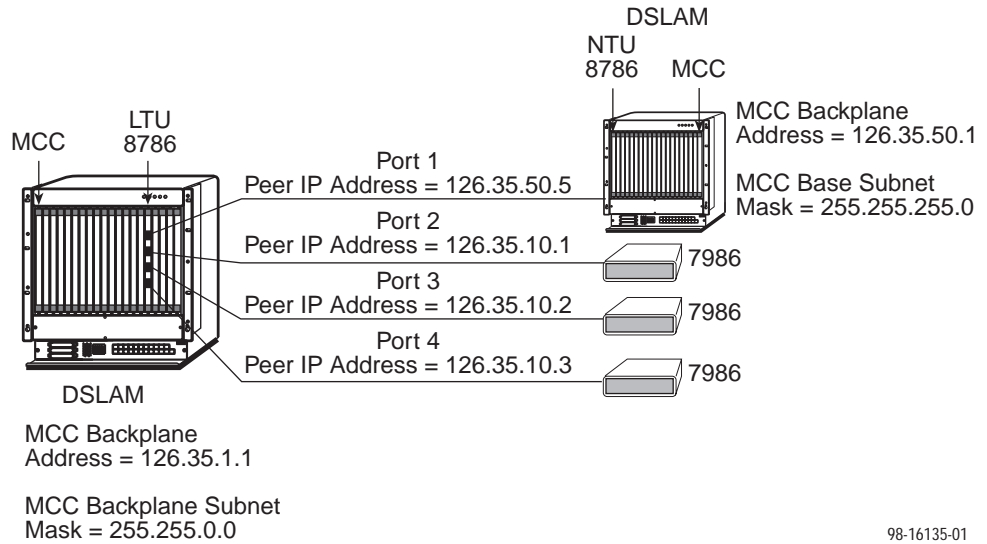
The 8786 Termination Unit is assigned an IP address and subnet through the DSLAM DSL Card Configuration menu. Once the address is assigned, you can use the 8786 Termination Unit's ATI to assign:

- Peer IP addresses to the four MSDSL ports. These addresses are used as the IP addresses of the remote units. See Table A-1, *Network Interface Options*, in Appendix A, *Configuration Option Tables*.
- An IP address for each NMS. For SNMP IP configuration options, see Table A-6, *SNMP Traps Options*, Table A-7, *General SNMP Management Options*, and Table A-8, *SNMP NMS Security Options*, in Appendix A, *Configuration Option Tables*.
- An IP address for the TFTP server you wish to use to upload and download configurations. See *Configuration Loader* in Chapter 3, *Initial Startup and Configuration*.

Review the following information in preparation for selecting an IP addressing scheme.

- Any legal host address is allowed for a given subnet. The address choice within the subnet is arbitrary.
- A single route to a subnet is all that is needed to reach every device on a subnet. The 8786 Termination Unit's routing table supports a maximum of 20 routes.

## IP Addressing Example



### Peer IP Address Assignments

- The Peer IP Address refers to the IP address of the unit configured as an NTU.
- The Peer IP Address is assigned by the LTU.

---

# Configuration Option Tables



---

## Overview

The tables in this appendix summarize the configuration options accessed when you select Configuration on the Main Menu. The configuration options are arranged into groups based upon functionality.

Select . . .	To Access the . . .	To Configure the . . .
Network	<a href="#">Network Interface Options</a> , Table A-1	E1 SDSL network interface Ports 1–2.
G.703 Interface	<a href="#">G.703 Interface Options</a> , Table A-2	G.703 interface 1–2.
Copy Ports	<a href="#">Copy Port Options</a> , Table A-3	E1 SDSL network and G.703 DTE interface ports by copying options from port to port.
System	<a href="#">System Options</a> , Table A-4	General system options of the unit.
Management and Communication	<ul style="list-style-type: none"><li>■ <a href="#">Telnet Session Options</a>, Table A-5</li><li>■ <a href="#">SNMP Traps Options</a>, Table A-6</li><li>■ <a href="#">General SNMP Management Options</a>, Table A-7</li><li>■ <a href="#">SNMP NMS Security Options</a>, Table A-8</li></ul>	Management support of the unit through SNMP and Telnet.

### NOTE:

All changes to configuration options must be saved. Refer to [Saving Configuration Options](#) in Chapter 3, *Initial Startup and Configuration*.

## Network Interface Options Menu

For Network Interface Options, refer to Table A-1. To access the Network Interface Options screen, follow this menu selection sequence:

*Main Menu* → *Configuration* → *Current Configuration* → *Network*

```

main/config/network
Slot 4
Port 3
Hotwire
Model: 8786

NETWORK INTERFACE OPTIONS

Margin Threshold:          -3db
Excessive Error Rate Threshold: 1E-6
AutoRate                  Disable
DSL Line Rate             400 Kbps

Peer IP Address:          111.255.255.000 Clear

Circuit Identifier: _____ Clear

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

**Table A-1. Network Interface Options (1 of 2)**

<b>Margin Threshold</b>
Possible Settings: <b>-5db, -4db, -3db, -2db, -1db, 0db, 1db, 2db, 3db, 4db, 5db, 6db, 7db, 8db, 9db, 10db</b> Default Setting: <b>0db</b>
Determines the level, expressed in decibels, at which a signal-to-noise margin condition is recognized. <b>-5db to 10db</b> – Sets the margin threshold to this value.
<b>Excessive Error Rate Threshold</b>
Possible Settings: <b>1E-4, 1E-5, 1E-6, 1E-7, 1E-8, 1E-9</b> Default Setting: <b>1E-6</b>
Determines the error rate at which an excessive error rate (EER) condition is recognized. The rate is the ratio of the number of CRC errors to the number of bits received in a certain period.
<b>AutoRate</b>
Possible Settings: <b>Enable, Disable</b> Default Setting: <b>Disable</b>
Specifies whether the DSL line will automatically train up to the best rate or if the line rate will be user selectable. <ul style="list-style-type: none"> <li>■ AutoRate is only available when the unit is configured as an LTU.</li> </ul> <b>Enable</b> – The LTU is set to adjust at the best line rate. <b>Disable</b> – The LTU Line rate is user selectable and is based on the DSL Line Rate selected.

**Table A-1. Network Interface Options (2 of 2)**

<b>DSL Line Rate</b>
Possible Settings: <b>400, 528, 784, 1040, 1552, 2064</b> Default Setting: <b>2064</b>
Specifies the DSL line rate of the unit. <ul style="list-style-type: none"> <li>■ DSL Line Rate is only available when the unit is configured as an LTU and AutoRate is disabled (unit is in fixed rate).</li> </ul> <p><b>400</b> – The DSL Line rate is 400 kbps.  <b>528</b> – The DSL Line rate is 528 kbps.  <b>784</b> – The DSL Line rate is 784 kbps.  <b>1040</b> – The DSL Line rate is 1040 kbps.  <b>1552</b> – The DSL Line rate is 1552 kbps.  <b>2064</b> – The DSL Line rate is 2064 kbps.</p> <p>NOTE: For associated payload rates refer to Table 3-1, <b>Fixed Rate Payload Rates and DSL Line Rates</b>, in Chapter 3, <i>Initial Startup and Configuration</i>.</p>
<b>Peer IP Address (LTU Only)</b>
Possible Settings: <b>000.000.000.001 – 223.255.255.255, Clear</b> Default Setting: <b>000.000.000.001</b>
Specifies the peer IP address providing the remote management link on the DSL loop. The Peer IP Address is only available when the unit is configured as an LTU. <p><b>Address Field – (000.000.000.001 – 223.255.255.255)</b> – Enter an address for the peer unit. The range for the first byte is 000 to 223, with the exception of 127. The range for the remaining three bytes is 000 to 255. The IP address must be in the same subnet as the MCC backplane address.</p> <p><b>Clear</b> – Clears the IP address and sets to all zeros.</p>
<b>Circuit Identifier</b>
Possible Settings: <b>[ASCII Text], Clear</b> Default Setting: [blank]
Uniquely identifies the circuit number of the transmission vendor's DSL line for troubleshooting purposes. <p><b>[ASCII Text]</b> – Enter a maximum of 128 characters. All printable ASCII characters except ^ (caret) are allowed.</p> <p><b>Clear</b> – Clears the field.</p>

## G.703 Interface Options

For G.703 Interface Options, refer to Table A-2. To access the G.703 Interface Options screen, follow this menu selection sequence:

*Main Menu → Configuration → Load Configuration From → G.703*

```

main/config/G.703
Slot: 4
Port: 2
Hotwire
Model: 8786

G.703 INTERFACE OPTIONS

Port Status:          Enable
Line Coding:          HDB3
Line Framing:         noCRC4
Time Slot 16:         Signaling
Send (AIS) on Network Failure: Enable
Primary Clock Source: G703

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

**Table A-2. G.703 Interface Options (1 of 2)**

Port Status
Possible Settings: <b>Enable, Disable</b> Default Setting: <b>Enable</b>
Determines whether the port can be configured and used.  <b>Enable</b> – The port can be configured and used.  <b>Disable</b> – The port cannot be configured or used. Configuration fields for the port are inaccessible, no alarms or traps associated with the port are generated, and the LED associated with the port is OFF.
Line Coding
Possible Settings: <b>AMI, HDB3</b> Default Setting: <b>HDB3</b>
Specifies the line coding format to be used by the G.703 interface.  <b>AMI</b> – Indicates the line coding format used by the G.703 interface is Alternate Mark Inversion (AMI).  <b>HDB3</b> – Indicates the line coding format used by the G.703 interface is HDB3.

Table A-2. G.703 Interface Options (2 of 2)

Line Framing (LTU Only)
Possible Settings: <b>CRC4, noCRC4</b> Default Setting: <b>noCRC4</b>
Specifies the framing format to be used by the G.703 interface. <ul style="list-style-type: none"> <li>■ Line Framing is only available when the unit is configured as an LTU, AutoRate is disabled, and the DSL Line rate is 2064 kbps. Otherwise the noCRC4 framing format is used. The NTU is automatically configured to match the framing format used by the LTU.</li> </ul> <p><b>CRC4</b> – CRC4 framing formatting is used for transmitted and received data over the G.703 Interface.</p> <p><b>noCRC4</b> – Non-CRC4 framing format is used for transmitted and received data over the G.703 Interface.</p>
Time Slot 16
Possible Settings: <b>Signaling, Data</b> Default Setting: <b>Signaling</b>
Specifies whether the G.703 interface is used for voice or data. <p><b>Signaling</b> – Timeslot 16 contains signaling information (the unit is in voice mode).</p> <p><b>Data</b> – Timeslot 16 contains data (the unit is in data mode).</p> <p>NOTE: For associated DSL line rates and payload rates refer to Table 3-1, <b>Fixed Rate Payload Rates and DSL Line Rates</b>, in Chapter 3, <i>Initial Startup and Configuration</i>.</p>
Send (AIS) on Network Failure
Possible Settings: <b>Enable, Disable</b> Default Setting: <b>Enable</b>
Specifies the action taken on the signal transmitted to the G.703 when a valid signal cannot be recovered from the network interface (LOS or OOF). <p><b>Enable</b> – An Alarm Indication Signal (AIS) is sent to the DTE in the event an LOS or continuous OOF condition exists on the network interface.</p> <p><b>Disable</b> – The failed signal on the interface is sent to the DTE in the event an LOS or continuous OOF condition exists on the network interface.</p>
Primary Clock Source
Possible Settings: <b>Internal, G.703</b> Default Setting: <b>Internal</b>
Determines the primary clock source for the 8786 Termination Unit. <p><b>Internal</b> – The clock source is derived from the internal oscillator.</p> <p><b>G703</b> – Specifies the unit's G.703 interface as primary clock source.</p>

## Copy Port Options

You can copy the configuration options of G.703 interface and DSL loop to another using the Copy Ports screen. For Copy Ports options, refer to Table A-3. To access the Copy Ports screen, follow this menu selection sequence:

*Main Menu → Configuration → Load Configuration From → Copy Ports*

```

main/config/copy
slot 4
Hotwire
Model: 8786

COPY PORTS

From: Port n:
To: Port y:

Perform Copy
Perform Copy Then Increment

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

**Table A-3. Copy Ports Options**

<b>From: Port <i>n</i></b>
Possible Settings: <b>1, 2</b> Default Setting: <b>1</b>
Controls the source of the configuration options. <b>1 to 2</b> – The configuration of the selected port is copied.
<b>To: Port <i>y</i></b>
Possible Settings: <b>1, 2, All</b> Default Setting: <b>2</b>
Controls the target of the configuration options. <b>1 to 2</b> – The configuration of the selected port is replaced. If Perform Copy Then Increment is selected, the port number is incremented by 1 after the copy. <b>All</b> – The configurations of all ports are replaced by the configuration of the selected From: Port.
NOTE: Peer IP Address and Circuit Identifier are <i>not</i> copied.

## System Options

For System Options, refer to Table A-4. To access the System Options screen, follow this menu selection sequence:

*Main Menu → Configuration → Load Configuration From → System*

```

main/config/system                               Hotwire
slot 4                                           Model: 8786

                                SYSTEM OPTIONS

                                DSL Mode:          LTU
                                Test Timeout:       Enable
                                Test Duration (min): 10
                                G.703 Line Termination 120 Ohm

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

**Table A-4. System Options (1 of 2)**

<b>DSL Mode</b>
Possible Settings: <b>LTU, NTU</b> Default Setting: <b>LTU</b>
Controls whether the unit is configured as a control unit or tributary unit. <b>LTU</b> – The unit is configured as a control unit (Line Termination Unit). <b>NTU</b> – The unit is configured as a tributary unit (Network Termination Unit). This unit will request its IP address from the LTU during establishment of the PPP link. NOTE: Changing this option will reset the card.
<b>Test Timeout</b>
Possible Settings: <b>Enable, Disable</b> Default Setting: <b>Enable</b>
Allows tests to end automatically. The feature should be enabled when the unit is remotely managed, so that control can be regained after a test is accidentally executed. <b>Enable</b> – Loopback and pattern tests end when test duration is reached. <b>Disable</b> – Tests run until manually terminated from the Network Tests screen or remotely (network initiated tests). Refer to <i>Running Network Tests</i> in Chapter 5, <i>Testing</i> .
<b>Test Duration (min)</b>
Possible Settings: <b>1–120</b> Default Setting: <b>10</b>
Number of minutes for a test to be active before automatically ending. <ul style="list-style-type: none"> <li>■ Test Duration (min) option appears when Test Timeout is enabled.</li> </ul> <b>1 to 120</b> – Amount of time in minutes for a test to run before terminating.

**Table A-4. System Options (2 of 2)**

<b>G.703 Line Termination</b>
Possible Settings: <b>75 ohms, 120 ohms</b> Default Setting: <b>120 ohms</b>
Specifies the impedance of the G.703 interface <b>75 ohms</b> – The G.703 interface impedance is 75 ohms unbalanced. <b>120 ohms</b> – The G.703 interface impedance is 120 ohms balanced.

## Management and Communication Options Menu

The Management and Communication Menu allows you to access the following:

- [Telnet Session Options](#), Table A-5
- [SNMP Trap Options](#), Table A-6
- [General SNMP Management Options](#), Table A-7
- [SNMP NMS Security Options](#), TableA-8

### Telnet Session Options

To access the Telnet Session Options screen, follow this menu selection sequence:

*Main Menu → Configuration → Load Configuration From → Management and Communication → Telnet Session*

```

main/config/management/telnet
slot 4
Hotwire
Model: 8786

TELNET SESSION OPTIONS

Telnet Session:           Enable
Telnet Login Required:    Enable
Session Access Level:    Administrator
Inactivity Timeout:      Enable
Disconnect Time (Minutes) 5

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

**Table A-5. Telnet Session Options**

<b>Telnet Session</b>
Possible Settings: <b>Enable, Disable</b> Default Setting: <b>Enable</b>
Specifies if the 8786 Termination Unit will respond to a Telnet session request from a Telnet client on an interconnected IP network. <b>Enable</b> – Allows Telnet sessions between the unit and a Telnet client. <b>Disable</b> – No Telnet sessions allowed.
<b>Telnet Login Required</b>
Possible Settings: <b>Enable, Disable</b> Default Setting: <b>Disable</b>
Specifies whether a user ID and password are required to access to the ATI through a Telnet session. Login IDs are created with a password and access level. Refer to <i>Creating a Login</i> in Chapter 7, <i>Security</i> . <b>Enable</b> – Security is enabled. When access is attempted via Telnet, the user is prompted for a Login ID and password. <b>Disable</b> – No Login required for a Telnet session.
<b>Session Access Level</b>
Possible Settings: <b>Administrator, Operator</b> Default Setting: <b>Administrator</b>
The Telnet session access level is interrelated with the access level of the Login ID. Refer to <i>ATI Access Levels</i> in Chapter 7, <i>Security</i> , for more information. <b>Administrator</b> – This is the higher access level, permitting full control of the 8786 Termination Unit. Access level is determined by the Login ID. If Telnet Login Required is disabled, the session access level is Administrator. <b>Operator</b> – This is the lower access level, permitting read-only access to status and configuration screens.
<b>Inactivity Timeout</b>
Possible Settings: <b>Enable, Disable</b> Default Setting: <b>Disable</b>
Provides automatic logoff of a Telnet session. <b>Enable</b> – The Telnet session terminates automatically after the Disconnect Time. <b>Disable</b> – A Telnet session will not be closed due to inactivity.
<b>Disconnect Time (Minutes)</b>
Possible Settings: <b>1–60</b> Default Setting: <b>5</b>
Number of minutes of inactivity before a Telnet session terminates automatically. Timeout is based on no keyboard activity. <ul style="list-style-type: none"> <li>■ Disconnect Time (minutes) option appears when Inactivity Timeout is enabled.</li> </ul> <b>1 to 60</b> – The Telnet session is closed after the selected number of minutes.

## SNMP Traps Options

SNMP configuration options allow you to specify the information necessary to support the Model 8786 termination unit SNMP traps. To access the SNMP Traps Options screen, follow this menu selection sequence:

*Main Menu → Configuration → Load Configuration From → Edit → Management and Communication → SNMP Traps*

```

main/config/management/trap                               Hotwire
Slot: 4                                                    Model: 8786

                                SNMP TRAPS OPTIONS

SNMP Traps:           Enable           Number of Trap Managers: 5

NMS 1 IP Address: 135.014.040.001 Clear
NMS 2 IP Address: 135.014.003.027 Clear
NMS 3 IP Address: 135.014.001.008 Clear
NMS 4 IP Address: 135.014.002.024 Clear
NMS 5 IP Address: 204.128.146.035 Clear

General Traps:           Both
Enterprise Specific Traps: Disable
Link Traps:              Both
Link Traps Interfaces:   All

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

**Table A-6. SNMP Traps Options (1 of 3)**

<b>SNMP Traps</b>
Possible Settings: <b>Enable, Disable</b> Default Setting: <b>Disable</b>
Controls the generation of SNMP trap messages. The options for addresses and types of traps are located in this table. <b>Enable</b> – SNMP trap messages are sent out to SNMP managers. <b>Disable</b> – No SNMP trap messages are sent out.
<b>Number of Trap Managers</b>
Possible Settings: <b>1, 2, 3, 4, 5</b> Default Setting: <b>1</b>
Sets the number of SNMP management systems that will receive SNMP traps. <b>1 to 5</b> – Number of trap managers. An NMS IP address is required for each manager.

Table A-6. SNMP Traps Options (2 of 3)

NMS <i>n</i> IP Address
Possible Settings: <b>000.000.000.000 – 223.255.255.255, Clear</b> Default Setting: <b>000.000.000.000</b>
Specifies the Internet Protocol address used to identify each SNMP trap manager. <b>000.000.000.000 – 223.255.255.255</b> – Enter an address for each SNMP trap manager. The range for the first byte is 000 to 223, with the exception of 127. The range for the remaining three bytes is 000 to 255. <b>Clear</b> – Clears the IP address and sets to all zeros.
NMS <i>n</i> Destination (NTU Only)
Possible Settings: <b>IMC, DSL1, DSL2</b> Default Setting: <b>IMC</b>
Provides the network destination path of each trap manager. <b>IMC</b> – The Internal Management Channel (IMC) is the default network destination. This is the management interface to the MCC card in the DSLAM. <b>DSL1 to DSL2</b> – The specified port is the network destination.
General Traps
Possible Settings: <b>Disable, Warm, AuthFail, Both</b> Default Setting: <b>Both</b>
Determines which SNMP traps are sent to each trap manager. <b>Disable</b> – No general trap messages are sent. <b>Warm</b> – Sends trap message for <i>warmStart</i> events. <b>AuthFail</b> – Sends trap message for <i>authenticationFailure</i> events. <b>Both</b> – Sends both trap messages. NOTE: Refer to Appendix B, <i>Standards Compliance for SNMP Traps</i> .
Enterprise Specific Traps
Possible Settings: <b>Enable, Disable</b> Default Setting: <b>Disable</b>
Determines if SNMP traps are generated for enterprise-specific events. <b>Enable</b> – SNMP traps are generated for <i>enterpriseSpecific</i> events. NOTE: Refer to <i>Enterprise Specific Traps</i> in Appendix B, <i>Standards Compliance for SNMP Traps</i> . <b>Disable</b> – No enterprise-specific event traps are sent.

**Table A-6. SNMP Traps Options (3 of 3)**

<b>Link Traps</b>
Possible Settings: <b>Disable, Up, Down, Both</b> Default Setting: <b>Both</b>
Determines if SNMP traps are generated for link up and link down for one of the communication interfaces.  <b>Disable</b> – No <i>linkUp</i> or <i>linkDown</i> SNMP traps are generated.  <b>Up</b> – A <i>linkUp</i> trap is generated when the 8786 Termination Unit recognizes that one of the communication interfaces is operational.  <b>Down</b> – A <i>linkDown</i> trap is generated when the 8786 Termination Unit recognizes a failure in one of the communication interfaces.  <b>Both</b> – Sends trap messages for detection of both <i>linkUp</i> and <i>linkDown</i> .  NOTE: Refer to <i>linkUp and linkDown</i> in Appendix B, <i>Standards Compliance for SNMP Traps</i> .
<b>Link Trap Interfaces</b>
Possible Settings: <b>Network, G.703, All</b> Default Setting: <b>All</b>
Determines if the SNMP <i>linkUp</i> , SNMP <i>linkDown</i> , and interface-related <i>enterpriseSpecific</i> traps are generated for the network DSL interface and/or G.703 interface (DTE).  <b>Network</b> – SNMP trap messages are generated for the DSL network interface.  <b>G.703</b> – SNMP trap messages are generated for the G.703 interface.  <b>All</b> – SNMP trap messages are generated for the DSL network interface and the G.703 interface.

## General SNMP Management Options

SNMP configuration options allow you to specify the information necessary to support the Termination Unit General SNMP functionality. To access the General SNMP Management Options screen, follow this menu selection sequence:

*Main Menu → Configuration → Load Configuration From → Edit → Management and Communication → SNMP → General SNMP Management*

```

main/config/management/SNMP
Slot: 4
Hotwire
Model: 8786

GENERAL SNMP MANAGEMENT OPTIONS

SNMP Management:  Enable_

Community Name 1:  Public___
Name 1 Access:    Read/Write_
Community Name 2:  Public___
Name 2 Access:    Read/Write_

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

**Table A-7. General SNMP Management Options (1 of 2)**

<b>SNMP Management</b>
Possible Settings: <b>Enable, Disable</b> Default Setting: <b>Disable</b>
Enables or disables the SNMP management features. <b>Enable</b> – Enables SNMP management capabilities. <b>Disable</b> – Disables SNMP management capabilities.
<b>Community Name 1</b>
Possible Settings: <b>ASCII text field, Public</b> Default Text: <b>Public</b>
Identifies the name of the community allowed to access the unit's MIB. The community name must be supplied by an external SNMP manager when that manager attempts to access an object in the MIB. <b>Text Field</b> – Enter or edit a community name. <b>Clear</b> – Clears the community name field.

**Table A-7. General SNMP Management Options (2 of 2)**

<b>Name 1 Access</b>
Possible Settings: <b>Read, Read/Write</b> Default Setting: <b>Read</b>
Determines the access level for Community Name 1. <b>Read</b> – Allows read-only access (get) for Community Name 1. <b>Read/Write</b> – Allows read/write access (get) for Community Name 1.
<b>Community Name 2</b>
Possible Settings: <b>ASCII text field, Public</b> Default Text: <b>Public</b>
Identifies the name of the second community allowed to access the unit's MIB. The community name must be supplied by an external SNMP manager when that manager attempts to access an object in the MIB. <b>Text Field</b> – Enter or edit a community name. <b>Clear</b> – Clears the community name field.
<b>Name 2 Access</b>
Possible Settings: <b>Read, Read/Write</b> Default Setting: <b>Read</b>
Determines the access level for Community Name 2. <b>Read</b> – Allows read-only access (get) for Community Name 2. <b>Read/Write</b> – Allows read/write access (get/set) for Community Name 2.

## SNMP NMS Security Options

SNMP configuration options allow you to specify the information necessary to support the Termination Unit SNMP NMS Security. To access the SNMP NMS Security Options screen, follow this menu selection sequence:

*Main Menu → Configuration → Load Configuration From → Edit → Management and Communication → SNMP → Security*

```

main/config/management/security                               Hotwire
Slot: 4                                                       Model: 8786

                               SNMP NMS SECURITY OPTIONS

                               NMS IP Validation:  Enable
                               Number of Managers:  2

NMS 1 IP Address: 135.014.040.001 Clear   Access Type: Read/Write
NMS 2 IP Address: 135.014.003.027 Clear   Access Type: Read/Write
NMS 3 IP Address: 135.014.001.008 Clear   Access Type: Read
NMS 4 IP Address: 135.014.002.024 Clear   Access Type: Read
NMS 5 IP Address: 204.128.146.035 Clear   Access Type: Read

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

**Table A-8. SNMP NMS Security Options (1 of 2)**

<b>NMS IP Validation</b>
Possible Settings: <b>Enable, Disable</b> Default Setting: <b>Disable</b>
Specifies whether security checking is performed on the IP address of SNMP management systems attempting to access the node.  <b>Enable</b> – Security checking is performed on the IP address of SNMP management systems attempting to access the node. <b>Disable</b> – No security checking is performed.
<b>Number of Managers</b>
Possible Settings: <b>1, 2, 3, 4, 5</b> Default Setting: <b>1</b>
Specifies the number of SNMP management systems that can send SNMP messages. <b>1 to 5</b> – Number of trap managers. An NMS IP address is required for each manager.

**Table A-8. SNMP NMS Security Options (2 of 2)**

<b>NMS <i>n</i> IP Address</b>
Possible Settings: <b>000.000.000.000 – 223.255.255.255, Clear</b> Default Setting: <b>000.000.000.000</b>
Specifies the Internet Protocol address used to identify each SNMP manager. <b>000.000.000.000 – 223.255.255.255</b> – Enter an address for each SNMP manager. The range for the first byte is 000 to 223, with the exception of 127. The range for the remaining three bytes is 000 to 255. <b>Clear</b> – Clears the IP address and sets to all zeros.
<b>Access Level</b>
Possible Settings: <b>Read, Read/Write</b> Default Setting: <b>Read</b>
Determines the access level allowed for an authorized NMS when IP address validation is being performed. <b>Read</b> – Allows read-only access (get) to the accessible objects in the MIB for this device. <b>Read/Write</b> – Allows read/write access (get/set) to the accessible objects in the MIB for this device.

---

# Standards Compliance for SNMP Traps

# B

---

## SNMP Traps

This section describes the unit's compliance with SNMP standards and any special operational features for the SNMP traps supported. The unit supports the following traps:

- warmStart
- authenticationFailure
- linkUp
- linkDown

### warmStart

SNMP Trap	Description	Possible Cause
warmStart	The unit has reinitialized itself.  The trap is sent after the unit resets and stabilizes.  There are no variable-bindings.	<ul style="list-style-type: none"><li>■ Reset command.</li><li>■ Power disruption.</li></ul>

### authenticationFailure

SNMP Trap	Description	Possible Cause
authenticationFailure	Failed attempts to access the unit.  There are no variable-bindings.	Three unsuccessful attempts were made to enter a correct login/password combination.

## linkUp and linkDown

The link SNMP traps are:

- **linkUp** – The unit recognizes that one of the communication interfaces is operational.
- **linkDown** – The unit recognizes that one of the communication interfaces is not operational.

The network and synchronous port interfaces (physical sublayer) are represented by an entry in the MIB-II interfaces table and supported by the DS1 MIB.

The following list describes the conditions that define linkUp and linkDown:

### linkUp/Down Variable-Bindings

- ifIndex (RFC 1573)

This object provides the index into the ifTable and potentially into tables in other MIBs. The values of ifIndex are the same for all models, although not all indexes are supported for each model.

The ifIndex included with the trap consists of the slot number times 1000, plus:

  - 2 HDSL E1 Interface, Port 1
  - 3 HDSL E1 Interface, Port 2
  - 6 G.703, Port 1
  - 7 G.703, Port 2
- ifAdminStatus (RFC 1573)

This object specifies the operational state of the interface:

  - up(1)

HDSL Network: DSL link is established.  
G.703: No alarm condition exists.
  - down(2)

HDSL Network: DSL link is not established.  
G.703: An alarm condition exists.
  - testing(3)

A test is active on the interface.
- ifOperStatus (RFC 1573)

This object contains the same value as ifAdminStatus.
- ifType (RFC 1573)

This object is the type of interface:

  - e1(19)

Used for the G.703 E1 interface.

## Enterprise-Specific Traps

The enterpriseSpecific trap indicates that an enterprise-specific event has occurred. The Specific-trap field identifies the particular trap that occurred. The following table lists the enterprise-specific traps supported by the unit:

SNMP Trap	Description	Possible Cause
enterprisePrimaryClockFail(1)	A failure of the currently configured primary clock source for the unit has been detected.	The configured clock source is no longer operational. If the configured clock source is the internal clock, the possible cause may be due to a failure of one or more of the unit's hardware components.
enterprisePrimaryClockFailClear(101)	The Clock Fail condition has cleared.	—
enterpriseSelfTestFail(2)	A hardware failure of the unit is detected during the unit's self-test. The trap is generated after the unit completes initialization.	Failure of one or more of the unit's hardware components.
enterpriseDeviceFail(3)	An internal device failure.	Operating software has detected an internal device failure.
enterpriseTestStart(5)	A test is running.	At least one test has been started on an interface.
enterpriseConfigChange(6)	The configuration changed via the user interface. The trap is sent after 60 seconds have elapsed without another change. This suppresses the sending of numerous traps when multiple changes are made in a short period of time, as is typically the case when changing configuration options.	Configuration has been changed via the AT1.
enterpriseFallbackAutoRate(13)	The LTU, set to AutoRate enable, resynched at a lower rate when the line was restored after an LOS.	After a LOS condition the units trained up at a lower rate than the previous rate.
enterpriseFallbackAutoRateClear(113)	The fallback autorate condition has cleared and the units have resynched at the same rate.	The units automatically retrained at the same rate, were reset, or placed in fixed rate.
enterpriseTestStop(105)	All tests have been halted.	All tests have been halted on an interface.

There are no variable-bindings for enterpriseDeviceFail and enterpriseConfigChange. The variable-binding for enterpriseSelfTestFail is devSelfTestResults.

The following list describes the conditions that define enterpriseFallbackAutoRate and enterpriseFallbackAutoRateClear:

<b>enterpriseFallbackAutoRate Variable-Bindings</b>
<ul style="list-style-type: none"><li>■ ifIndex (RFC 1573) This object provides the index into the ifTable and potentially into tables in other MIBs. The values of ifIndex are the same for all models, although not all indexes are supported for each model. The ifIndex included with the trap consists of the slot number times 1000, plus:<ul style="list-style-type: none"><li>– 2 HDSL E1 Interface, Port 1</li><li>– 3 HDSL E1 Interface, Port 2</li><li>– 6 G.703, Port 1</li><li>– 7 G.703, Port 2</li></ul></li><li>■ ifAdminStatus (RFC 1573) This object specifies the operational state of the interface:<ul style="list-style-type: none"><li>– up(1) HDSL Network: DSL link is established. G.703: No alarm condition exists.</li><li>– down(2) HDSL Network: DSL link is not established. G.703: An alarm condition exists.</li><li>– testing(3) A test is active on the interface.</li></ul></li><li>■ ifOperStatus (RFC 1573) This object contains the same value as ifAdminStatus.</li><li>■ ifType (RFC 1573) This object is the type of interface:<ul style="list-style-type: none"><li>– e1(19) Used for the G.703 E1 interface.</li></ul></li></ul>

The tests that affect the enterpriseTestStart, enterpriseTestStop, and the variable-bindings are different for each particular interface. Diagnostic tests are only supported on the physical E1 network and user data port interfaces. The specific tests and variable-bindings are described in the following table:

Interface	enterpriseTestStart/Stop Variable-Bindings	Possible Cause
HDSL Network	<ul style="list-style-type: none"> <li>■ ifIndex (RFC 1573)</li> <li>■ ifAdminStatus (RFC 1573)</li> <li>■ ifOperStatus (RFC 1573)</li> <li>■ ifType (RFC 1573)</li> <li>■ ifTestType (RFC 1573)</li> </ul> <p>The following objects control tests in SNMP-managed devices:</p> <ul style="list-style-type: none"> <li>– noTest – Stops the test in progress.</li> <li>– testLoopLLB – Initiates a Local Loopback.</li> <li>– testLoopRLB – Initiates a Remote Loopback.</li> <li>– testSendMon511 – Initiates a Send and Monitor 511 test.</li> <li>– testSendLLBUp – Initiates an LLB Up message to the remote unit.</li> <li>– testSendLLBDown – Initiates an LLB Down message to the remote unit.</li> </ul>	<ul style="list-style-type: none"> <li>■ enterpriseTest Start – Any one of the following tests is active on the interface: <ul style="list-style-type: none"> <li>– Line Loopback</li> <li>– Repeater Loopback</li> <li>– Remote Line Loopback</li> <li>– Send and Monitor 511</li> </ul> </li> <li>■ enterpriseTest Stop – No tests currently running on the interface.</li> </ul>
G.703	<ul style="list-style-type: none"> <li>■ ifIndex (RFC 1573)</li> <li>■ ifAdminStatus (RFC 1573)</li> <li>■ ifOperStatus (RFC 1573)</li> <li>■ ifTestType (RFC 1573)</li> </ul> <p>The following objects control tests in SNMP-managed devices:</p> <ul style="list-style-type: none"> <li>– noTest – Stops the test in progress.</li> <li>– testLoopExternalDTE</li> </ul>	



---

# Connector Pin Assignments

# C

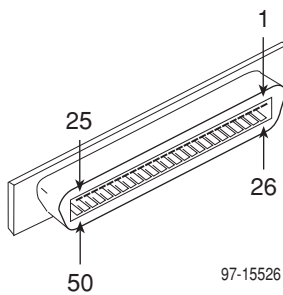
---

## Overview

The following sections provide connector pin assignments for the:

- *Hotwire 8600 DSLAM Telco 50-pin Connector Pinouts for DSL Loops*
- *Hotwire 8800 DSLAM Telco 50-pin Connector Pinouts for DSL Loops*
- *Hotwire 8786 Front Panel 50-pin Connector Pinouts*

## Hotwire 8600 DSLAM Telco 50-pin Connector Pinouts for DSL Loops



The Telco 50-pin LINE receptacle on the front panel of the 8600 DSLAM provides the 2-wire loop interface from each M/HDSL port to the MDF. The following table lists the pin assignments for each of these interfaces.

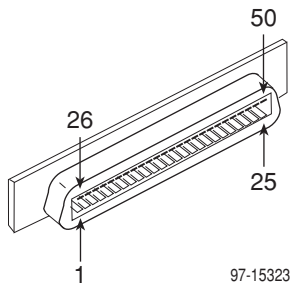
**NOTE:**

When the 8600 chassis is the base chassis, the MCC is installed in Slot 1 and the Tip and Ring wiring for Slot 1 is not active.

Also, Pins 13 through 25 and 38 through 50 of all Hotwire 8600 chassis are not used.

CONNECTOR (DSL Slot, Port Number)	CONNECTOR PINS (Tip, Ring)
Slot 1, Port 1 (TX)	1, 26
Slot 1, Port 1 (RX)	2, 27
Slot 1, Port 2 (TX)	3, 28
Slot 1, Port 2 (RX)	4, 29
Slot 2, Port 1 (TX)	5, 30
Slot 2, Port 1 (RX)	6, 31
Slot 2, Port 2 (TX)	7, 32
Slot 2, Port 2 (RX)	8, 33
Slot 3, Port 1 (TX)	9, 34
Slot 3, Port 1 (RX)	10, 35
Slot 3, Port 2 (TX)	11, 36
Slot 3, Port 2 (RX)	12, 37

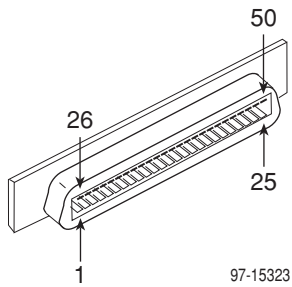
## Hotwire 8800 DSLAM Telco 50-pin Connector Pinouts for DSL Loops



The three Telco 50-pin LINES connectors on the 8800 DSLAM Interface Module provide the 4-wire loop interface from each DSL port to the MDF. The following table lists the pin assignments for each of these interfaces. Note that Pins 25 and 50 are *not* used.

CONNECTOR 1 Slots 1–6 8786 Port Number	CONNECTOR 2 Slots 7–12 8786 Port Number	CONNECTOR 3 Slots 13–18 8786 Port Number	CONNECT. PINS (Tip, Ring)
Card 1, Port 1 (TX)	Card 7, Port 1 (TX)	Card 13, Port 1 (TX)	1, 26
Card 1, Port 1 (RX)	Card 7, Port 1 (RX)	Card 13, Port 1 (RX)	2, 27
Card 1, Port 2 (TX)	Card 7, Port 2 (TX)	Card 13, Port 2 (TX)	3, 28
Card 1, Port 2 (RX)	Card 7, Port 2 (RX)	Card 13, Port 2 (RX)	4, 29
Card 2, Port 1 (TX)	Card 8, Port 1 (TX)	Card 14, Port 1 (TX)	5, 30
Card 2, Port 1 (RX)	Card 8, Port 1 (RX)	Card 14, Port 1 (RX)	6, 31
Card 2, Port 2 (TX)	Card 8, Port 2 (TX)	Card 14, Port 2 (TX)	7, 32
Card 2, Port 2 (RX)	Card 8, Port 2 (RX)	Card 14, Port 2 (RX)	8, 33
Card 3, Port 1 (TX)	Card 9, Port 1 (TX)	Card 15, Port 1 (TX)	9, 34
Card 3, Port 1 (RX)	Card 9, Port 1 (RX)	Card 15, Port 1 (RX)	10, 35
Card 3, Port 2 (TX)	Card 9, Port 2 (TX)	Card 15, Port 2 (TX)	11, 36
Card 3, Port 2 (RX)	Card 9, Port 2 (RX)	Card 15, Port 2 (RX)	12, 37
Card 4, Port 1 (TX)	Card 10, Port 1 (TX)	Card 16, Port 1 (TX)	13, 38
Card 4, Port 1 (RX)	Card 10, Port 1 (RX)	Card 16, Port 1 (RX)	14, 39
Card 4, Port 2 (TX)	Card 10, Port 2 (TX)	Card 16, Port 2 (TX)	15, 40
Card 4, Port 2 (RX)	Card 10, Port 2 (RX)	Card 16, Port 2 (RX)	16, 41
Card 5, Port 1 (TX)	Card 11, Port 1 (TX)	Card 17, Port 1 (TX)	17, 42
Card 5, Port 1 (RX)	Card 11, Port 1 (RX)	Card 17, Port 1 (RX)	18, 43
Card 5, Port 2 (TX)	Card 11, Port 2 (TX)	Card 17, Port 2 (TX)	19, 44
Card 5, Port 2 (RX)	Card 11, Port 2 (RX)	Card 17, Port 2 (RX)	20, 45
Card 6, Port 1 (TX)	Card 12, Port 1 (TX)	Card 18, Port 1 (TX)	21, 46
Card 6, Port 1 (RX)	Card 12, Port 1 (RX)	Card 18, Port 1 (RX)	22, 47
Card 6, Port 2 (TX)	Card 12, Port 2 (TX)	Card 18, Port 2 (TX)	23, 48
Card 6, Port 2 (RX)	Card 12, Port 2 (RX)	Card 18, Port 2 (RX)	24, 49

## Hotwire 8786 Front Panel 50-pin DTE Connector Pinouts



The DTE connectors on the 8786 termination unit provide the 4-wire G.703 interface from each DSL port to the DTE. The following table lists the pin assignments for each of these interfaces.

G.703 Port	50-Pin Connector Pinout	Function
Port 2	30	Data Out (Ring)
	5	Data Out (Tip)
	29	Data In (Tip)
	4	Data In (Ring)
Port 1	27	Data Out (Ring)
	2	Data Out (Tip)
	26	Data In (Tip)
	1	Data In (Ring)

---

# Technical Specifications

# D

---

Specifications	Criteria*
<b>Size</b>	Length 10 inches (25.4 cm) Height 12.3 inches (31.1 cm) Width 0.8 inch (2.0 cm)
<b>Weight</b>	Approximately 1.3 lbs. (0.6 kg)
<b>Approvals</b> Safety Certifications	Refer to the equipment's label for approvals on product.
<b>Power</b>	The 8786 Termination Unit contains a DC-to-DC converter that requires -48V power input. The -48V power is distributed through the Hotwire DSLAM backplane. Maximum Power Dissipation = 19 watts
<b>Physical Environment</b> Operating temperature Storage temperature Relative humidity Shock and vibration	32° to 122° F (0° to 50° C) -4° F (-20° C) to 158° F (70° C) 5% to 85% (noncondensing) Withstands normal shipping and handling.
* Technical specifications are subject to change without notice.	



---

# Glossary

---

<b>511</b>	A random bit test 511 bytes in length.
<b>AMI</b>	Alternate Mark Inversion. A line coding technique used to accommodate the ones density requirements of E1 or T1 lines.
<b>ATI</b>	Asynchronous Terminal Interface. A menu-driven, VT100-compatible system for configuring and managing the termination unit.
<b>BPV</b>	Bipolar Violation. In a bipolar signal, a one (mark, pulse) which has the same polarity as its predecessor.
<b>bridged tap</b>	Any part of the local loop that is not in the direct talking path between the CO and the service user.
<b>CD</b>	Carrier Detect. The received line signal detector. V.24 circuit 109.
<b>CO</b>	Central Office/Central Site. The PSTN facility that houses one or more switches serving local telephone subscribers.
<b>COM port</b>	Communications port. A computer's serial communications port used to transmit to and receive data from a modem. The modem connects directly to this port.
<b>CP</b>	Customer Premises.
<b>CPE</b>	Customer Premises Equipment. Terminal equipment on the service user's side of the telecommunications network interface.
<b>CPU</b>	Central Processing Unit. The main or only computing device in a data processing system.
<b>CRC</b>	Cyclic Redundancy Check. A mathematical method of confirming the integrity of received digital data.
<b>CV</b>	Code Violation. Detected when using HDB3 coding format, this is equivalent to a BPV when using AMI coding.
<b>DCE</b>	Data Communications Equipment. The equipment that provides the functions required to establish, maintain, and end a connection. It also provides the signal conversion required for communication between the DTE and the network.
<b>DCLB</b>	Data Channel LoopBack. Loops the data received from the network interface, for all DS0 channels allocated to the selected port, back to the network.
<b>DSL</b>	Digital Subscriber Line. The non-loaded, local-loop copper connection between the customer and the first node within the network.
<b>DSLAM</b>	Digital Subscriber Line Access Multiplexer. A platform for DSL modems that provides high-speed data transmission over traditional twisted-pair wiring.
<b>DSR</b>	Data Set Ready. A signal from the modem to the DTE that indicates the modem is turned ON and connected to the DTE.
<b>DTE</b>	Data Terminal Equipment. The equipment, such as a computer or terminal, that provides data in the form of digital signals for transmission.
<b>DTLB</b>	Data Terminal LoopBack. Loopback mode that loops the data for a particular synchronous data port back to the port just before it is combined with the rest of the T1 data stream.

<b>E1</b>	A wideband digital interface operating at 2.048 Mbps, defined by ITU recommendations G.703 and G.704. It is used primarily outside North America.
<b>EER</b>	Excessive Error Rate. An error rate that is greater than the threshold that has been configured in the device.
<b>EOC</b>	Embedded Operations Channel. An in-band channel between DSL devices, used for 4 kbps management data.
<b>ES</b>	Errored Seconds. A second with one or more ESF error events (one or more CRC6 error events or OOFs).
<b>ESF</b>	Extended SuperFrame. The T1 transmission standard that specifies 24 frames as an extended superframe to be used for frame synchronization and to locate signaling bits.
<b>Ethernet</b>	A type of network that supports high-speed communication among systems. It is a widely implemented standard for LANs. All hosts are connected to a coaxial cable where they contend for network access using a Carrier Sense, Multiple Access with Collision Detection (CSMA/CD) paradigm.
<b>ETSI</b>	European Telecommunications Standardization Institute. An organization that produces technical standards in the area of telecommunications.
<b>factory defaults</b>	A predetermined set of configuration options containing the optimum settings for operation on asynchronous dial networks.
<b>FAS</b>	Frame Alignment Signal. A loss of signal (LOS) error detection.
<b>FAW</b>	Frame Alignment Word. A loss of synchronization error detection.
<b>FCC</b>	Federal Communications Commission. The Board of Commissioners that regulates all electrical communications that originate in the United States.
<b>FEBE</b>	Far-End Block Error. Block errors reported by remote equipment.
<b>frame relay</b>	A high-speed connection-oriented packet switching WAN protocol using variable-length frames.
<b>FTP</b>	File Transfer Protocol. A TCP/IP standard protocol that allows a user on one host to access and transfer files to and from another host over a network, provided that the client supplies a login identifier and password to the server.
<b>G.703</b>	An ITU recommendation for the physical and logical characteristics of hierarchical digital devices.
<b>G.704</b>	An ITU recommendation for synchronous frame structures.
<b>HDB3</b>	High Density Bipolar Three Zeros Substitution. A line coding technique used to accommodate the ones density requirements of E1 lines.
<b>IP</b>	Internet Protocol. An open networking protocol used for internet packet delivery.
<b>IP address</b>	Internet Protocol address. The address assigned to an internet host.
<b>kbps</b>	Kilobits per second. One kilobit is usually taken to be 1,024 bits.
<b>LAN</b>	Local Area Network. A privately owned and administered data communications network limited to a small geographic area.
<b>LED</b>	Light Emitting Diode. A light or status indicator that glows in response to the presence of a certain condition (e.g., an alarm).
<b>LLB</b>	Line LoopBack. A test in which the received signal on the network interface is looped back to the network without change.

---

<b>loopback</b>	A diagnostic procedure that sends a test message back to its origination point. Used to test various portions of a data link in order to isolate an equipment or data line problem.
<b>LOS</b>	Loss of Signal. The E1 line condition where there are no pulses.
<b>LTU</b>	Line Termination Unit. The control unit on the network end of a link. (The NTU is on the customer premises end.)
<b>Mbps</b>	Megabits per second. One megabit is 1,048,576 (1024 <sup>2</sup> ) bits.
<b>MCC</b>	Management Communications Controller. The DSLAM circuit card used to configure and monitor the DSLAM.
<b>MIB</b>	Management Information Base. A database of managed objects used by SNMP to provide network management information and device control.
<b>MIB II</b>	MIB Release 2. The current Internet-standard MIB, defined by RFC 1213.
<b>M/SDSL</b>	Multirate SDSL.
<b>MTSO</b>	Mobile Telephone Switching Office. A generic name for the main cellular switching center which supports multiple base stations.
<b>NMS</b>	Network Management System. A computer system used for monitoring and controlling network devices.
<b>NTU</b>	Network Termination Unit. The unit on the customer premises end of a link. (The LTU is on the network end.)
<b>OOF</b>	Out Of Frame. An error condition in which frame synchronization bits are in error.
<b>reset</b>	An initialization of the device that occurs at power-up or in response to a reset command.
<b>RLB</b>	Repeater LoopBack. Loops the signal being sent to the network back to the DTE Drop/Insert and data ports after it has passed through the framing circuitry of the device.
<b>router</b>	A device that connects LANs by dynamically routing data according to destination and available routes.
<b>SDSL</b>	Symmetrical Digital Subscriber Line. A technique for the use of an existing twisted-pair line that permits high bandwidth, bidirectional transmission.
<b>SES</b>	Severely Errored Seconds. Usually defined as a second during which a specific number of CRC errors was exceeded, or an OOF or other critical error occurred.
<b>SNMP</b>	Simple Network Management Protocol. Protocol for open networking management.
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol. The dominant protocol suite in the worldwide Internet, TCP allows a process on one machine to send data to a process on another machine using the IP. TCP can be used as a full-duplex or one-way simplex connection.
<b>Telnet</b>	Virtual terminal protocol in the Internet suite of protocols. Allows the user of one host computer to log into a remote host computer and interact as a normal terminal user of the remote host.
<b>TFTP</b>	Trivial File Transfer Protocol. A standard TCP/IP protocol that allows simple file transfer to and from a remote system without directory or file listing. TFTP is used where FTP is not available.
<b>TXD</b>	Transmit Data. Pin 2 of the EIA-232 interface that is used by the DTE to transmit data to the modem. Conversely, the modem uses Pin 2 to receive data from the DTE.
<b>UNIX</b>	An operating system developed at AT&T Bell Laboratories and since used as the basis of similar operating systems.
<b>WAN</b>	Wide Area Network. A network that spans a large geographic area.



---

# Index

---

## A

- Abort All Tests, 5-1
- access
  - SNMP, 7-4
  - to async terminal interface, 2-5
- access level
  - effective, 7-1
  - functions available for, 7-1
- administer login, 7-2
- AIS (Alarm Indication Signal), status message, 4-3
- Alarm, LED, 4-13
- ASCII, printable characters, 3-2
- ATI (Asynchronous Terminal Interface)
  - access, 2-1
  - defined, 1-2
  - exiting, 2-11
  - initiating session, 2-4
  - virtual function keys, 2-9
- authenticationFailure, B-1
- AutoRate, 3-6, A-2

## C

- cables, rear panel, C-1
- Card Failed
  - self-test result, 4-5
  - status message, 4-4
- Card Selection screen, 2-3
- Circuit Identifier, A-3
- Clock Failed, status message, 4-4
- Community Name , A-13, A-14
- Community Name 1, A-13
- Community Name 2, A-14
- community names, for SNMP, 7-4
- Configuring AutoRate, 3-6
- configuration
  - Copy Port Options, A-6
  - example, 1-3
  - G.703 Interface Options , A-4
  - General SNMP Management Options, A-13
  - Network Interface Options, A-2
  - option tables, A-1
  - SNMP Management, A-13

- SNMP NMS Security Options, A-13, A-15
- SNMP Trap Options, A-10
- System Options, A-7
- Telnet Session Options, A-8
- configuration changes, saving, 3-10
- Configuration Edit/Display, 3-5
- Configuration Loader, 3-8
- Configuration menu, 3-4
- configuration options
  - Copy Ports, A-6
  - G.703 Interface, A-4
- Copy Ports, A-6
- CPU Fail, self-test result, 4-5
- create login ID, 7-2
- customer configuration areas, 3-3

## D

- default configuration area, 3-3
- delete, Login ID, 7-4
- device
  - messages, 6-3– 6-4
  - name, 3-2
- dimensions, D-1
- Disconnect Time, for Telnet session, A-9
- documents, related, vi
- DOS, TFTP server on, 3-8
- download code, 3-11
- Download Failed, status message, 4-4
- DSL Line Rate, A-3
  - Fixed Rate, 3-7
- DSL Line Rates, 3-7
- DSL Port, LEDs, 4-13
- DSLAM
  - card selection, 2-3
  - defined, 1-2
  - exiting from session, 2-11
  - login, 2-2
- DTE loopback , 5-5

**E**

- EER (Excessive Error Rate) , status message, 4-3
- effective access level, 7-1
- ending an ATI session, 2-11
- enterprise, SNMP traps, B-3
- Enterprise Specific Traps, A-11
- environment requirements, D-1
- error messages, line 24, 6-3
- error statistics, 4-7
- Excessive Error Rate (EER) Threshold, A-2

**F**

- factory defaults, 3-3
- Failure, self-test result, 4-5
- features, 1-2
- firmware, download from server, 3-11

**G**

- G.703 Interface Impedance, A-8
- G.703 Interface Option settings, A-4
  - Line Coding Format, A-4
  - Line Framing, A-5
  - Primary Clock Source, A-5
  - Send (AIS) on Network Failure, A-5
  - Timeslot 16, A-5
- G.703 Interface Options, A-4
- General SNMP Traps Options, A-13
- General Traps, A-11

**H**

- health and status messages, 4-3

**I**

- identity, 3-2
- Impedance, A-8
- inactivity timeout, for Telnet session, A-9
- intended audience, v
- IP address
  - DSL peer, A-3
  - SNMP manager, 7-5
- IP addresses, 8-1
- IP addressing, example, 8-2

**K**

- keyboard functions, 2-8

**L**

- lamp test, 5-8
- LEDs, 4-12, 4-13
- Line Coding Format, A-4
- Line Framing , A-5
- Link Up, LEDs, 4-13
- link-layer protocols, 8-1
- linkUp and linkDown traps, B-2
- local line loopback (LLB), 5-3
- LOF (Loss Of Frame), status message, 4-3
- login, DSLAM, 2-2
- Login ID
  - access levels, 7-1
  - adding, 7-2
  - deleting, 7-4
- login ID, 7-1
- loopback, effect on LEDs, 4-13
- LOS (Loss Of Signal), status message, 4-3

**M**

- main menu, 2-4
- Management and Communication Options, A-8
- management port
  - access, 7-1
  - settings, 2-1
- Margin Threshold, A-2
- MCC, defined, 1-2
- Memory Fail, status, 4-5
- messages
  - alarm and device, 6-1
  - health and status, 4-3
  - line 24, 6-3
  - self-test results, 4-5
  - test status, 4-6
- MIB
  - general support, 1-4
  - support, 1-4
- monitoring, 4-1

**N**

- navigating the screens, 2-8
- Net Margin Threshold, status message, 4-3
- network, tests, 5-2
- G.703 Failed, self-test result, 4-5
- Network DSL Failed, self-test result, 4-5
- Network Interface Options, A-2
  - AutoRate, A-2
  - Circuit Identifier, A-3
  - DSL Line Rate, A-3
  - Excessive Error Rate Threshold, A-2
  - Margin Threshold, A-2
  - Peer IP Address, A-3
- NMS
  - SNMP access, 7-5
  - SNMP connectivity, 8-1
- no test active status message, 4-6

**O**

- OK, LED, 4-13
- OOF (Out Of Frame), status message, 4-3
- options, configuration tables, A-1
- overview
  - 8775 Termination Unit, 1-2
  - user's guide, v

**P**

- Passed, self-test result, 4-5
- Payload Rates, 3-7
- Peer IP Address, A-3
- performance statistics
  - DSL Network, 4-8
  - G.703, 4-10
- physical environment requirements, D-1
- pin assignments, C-1
- Port Status, A-4
- power requirements, D-1
- Primary Clock Source, A-5

**R**

- related documents, vi
- remote send line loopback, 5-6
- repeater loopback (RLB), 5-4
- reset, ATI, 3-11
- restore access to ATI, 3-11

**S**

- Save Configuration screen, 3-10
- saving option changes, 3-10
- screen, function keys, 2-9
- screens, for user interface, 2-1– 2-6
- SDSL Mode, A-7
- security, 7-1
- self-test results, 4-5
- Send and Monitor 511, 5-7
- Send Remote Line Loopback, 5-6
- size of card, D-1
- SNMP
  - system entries, 3-2
  - trap options, 6-2
  - traps, B-1
- SNMP Management Configuration, A-13
- SNMP management
  - general, 1-4
  - limiting access, 7-4
- SNMP NMS Security Options, A-13, A-15
- SNMP Trap Options, A-10
  - Enterprise Specific Traps, A-11
  - Link Trap Interfaces, A-12
  - Link Traps, A-12
  - NMS n Destination, A-11
  - NMS n IP Address, A-11, A-16
  - Number of Trap Managers, A-10
  - SNMP Traps, A-10
- SNMP Traps, enable/disable, A-10
- start-up, ATI, 2-1
- status, test messages, 4-6
- subnet, IP addresses, 8-1
- Sync Port, LEDs, 4-13
- system
  - device name fields, 3-2
  - LEDs, 4-13
- System Options, A-7
  - DSL Mode, A-7
  - Test Duration, A-7
  - Test Timeout, A-7

## T

- Telnet session
  - access level, A-9
  - enable/disable, A-9
  - login required, A-9
- telnet session access, 7-1
- Telnet Session Options
  - Disconnect Time (Minutes), A-9
  - inactivity timeout, A-9
  - Session Access Level, A-9
  - Telnet Login Required, A-9
  - Telnet Session, A-9
- telnet session options, A-8
- terminal port, direct connection, 2-1
- test
  - aborting, 5-9
  - DTE Loopback, 5-5
  - LED, 4-13
  - Line Loopback, 5-3
  - Remote Send Line Loopback, 5-6
  - Repeater Loopback, 5-4
  - Send and Monitor 511, 5-7
  - status messages, 4-6
  - terminating, 5-9
  - Test Duration, A-7
  - Test Timeout, A-7
- Test menu, 5-2
- testing, 5-1
- Time Slot 16, A-5
- timeout
  - Telnet session inactivity, A-9
  - Test, A-7
- SNMP Trap Support, 1-4
- traps, SNMP, 6-2, B-1
- troubleshooting, 6-5
  - DSL network performance statistics, 4-8
  - error statistics, 4-7
  - G.703 performance statistics, 4-10

## U

- UNIX, TFTP server on, 3-8
- user interface
  - access, 3-11
  - async terminal, 2-1
  - how to access, 2-1

## V

- virtual function keys, 2-9

## W

- warmStart, B-1
- weight of card, D-1