MODEL 7610 SNMP DSU

USER'S GUIDE

Document No. 7610-A2-GB20-10

November 1997

PARADYNE™

Notice

Trademarks

Warranty, Sales, and Service Information

Contact your sales or service representative directly for any help needed. For additional information concerning warranty, service, repair, spare parts, installation, documentation, or training, 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
  - — International, call 727-530-2340

Printed on recycled paper

Contents

3 Customizing the SNMP DSU

4 Security

5 IP Addressing

6 Monitoring the DSU

7 Testing

8 Messages and Troubleshooting

A Configuration Option Tables

B Worksheets

C MIB Descriptions

D Standards Compliance for SNMP Traps

E Cables and Pin Assignments

About This Guide

Document Purpose and Intended Audience

This guide contains information needed to set up, configure, and operate the Model 7610 SNMP DSU and is intended for installers and operators.

Document Summary

Section	Description
Chapter 1	*About the SNMP DSU.* Describes the DSU features and SNMP management capabilities with a typical configuration example.
Chapter 2	*Using the ATI.* Provides instructions for accessing the user interface and navigating the screens.
Chapter 3	*Customizing the SNMP DSU.* Provides procedures for setting up the user interface, device information, call setup, and DSU configuration steps.
Chapter 4	*Security.* Presents procedures for creating a login, setting the effective access levels, and controlling SNMP access.
Chapter 5	*IP Addressing.* Provides details regarding IP addresses with examples.
Chapter 6	*Monitoring the DSU.* Describes monitoring details about the LEDs, DSU status, and network statistics.
Chapter 7	*Testing.* Provides details about available tests and test setup.
Chapter 8	*Messages and Troubleshooting.* Provides information on ASCII alarms, SNMP traps, device messages, and troubleshooting.

Section	Description
Appendix A	*Configuration Option Tables.* Contains all configuration options, default settings, and possible settings.
Appendix B	*Worksheets.* Contains all the configuration options, default settings, and possible settings to use for planning.
Appendix C	*MIB Descriptions.* Provides all MIBs supported by the DSU.
Appendix D	*Standards Compliance for SNMP Traps.* Contains SNMP trap compliance details.
Appendix E	*Cables and Pin Assignments.* Contains connector and interface details.
Glossary	Defines acronyms and terms used in this document.
Index	Lists key terms, acronyms, concepts, and sections in alphabetical order.

Product-Related Documents

Document Number	Document Title
7610-A2-GN10	*Model 7610 SNMP DSU Startup Instructions*

To order additional product documentation, refer to the *Warranty, Sales, and Service Information* section on page A at the beginning of this User's Guide.

About the SNMP DSU

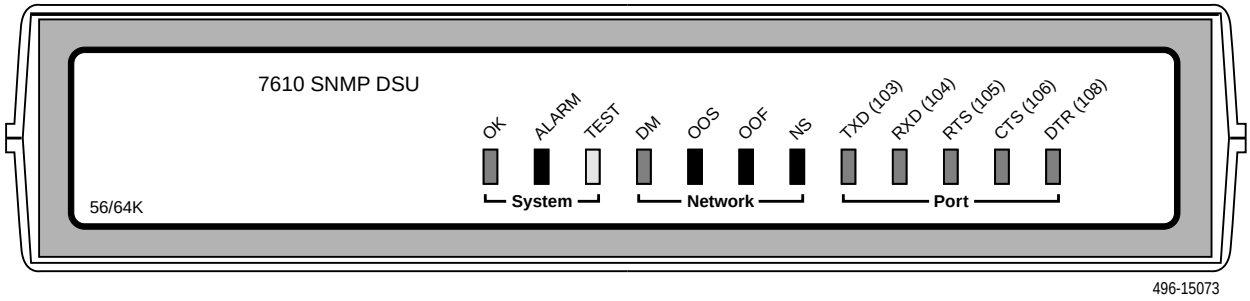
1

Model 7610 SNMP DSU Features

The SNMP DSU provides an interface between the customer premises equipment (CPE) and a DDS network. Its features include:

- **SNMP (Simple Network Management Protocol) Management.** Provides network management via an industry-standard SNMP management system.
- **In-band Management Channel (IMC).** Provides remote management via SNMP or Telnet session capability over the DDS network.
- **Async Terminal Interface (ATI).** Provides a menu-driven VT100-compatible interface for configuring and managing the DSU locally or remotely by Telnet session or External Modem.
- **Local Management.** Provides local management via an:
  - — Async terminal connection through the Terminal port
  - — NMS connection through the Management port
- **Remote Management.** Provides remote management:
  - — Out-of-band, using an external modem through the Terminal port or Management port
  - — Via Telnet through the Management port or the In-band Management Channel (IMC)
- **DDS Rates.** Operates at 56 and 64 kbps CC (clear channel).
- **LADS Operation (Local Area Data Set).** Operates at 56 and 64 kbps full-duplex (also called a limited distance modem).
- **Autorating of Line Rate.** Establishes the line rate from the network receive signal and automatically adjusts to the detected line rate.
- **Data Port Rates.** Supports the same rates as the DDS or LADS operating rates, except when the IMC is enabled.

- **Alarm Indication.** Activates front panel LEDs and provides the capability of attaching an ASCII terminal or printer to display/print alarm messages.



- **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.
- **Two Customer-Specified Configuration Storage Areas.** Allows quick access to alternate sets of configuration options.
- **Security.** Provides multiple levels of security, which prevents unauthorized access to the DSU.

SNMP Management Capabilities

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

MIB Support

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 DSU. MIB II is backward-compatible with MIB I.
- **RS-232-Like MIB (RFC 1659)** – Defines objects for managing RS-232-type interfaces (e.g., V.35, RS-422, RS-423, etc.) and supports synchronous data ports and management communication ports on the DSU.
- **Enterprise MIB** – Supports configuration, status, statistics, and tests on the DDS network interface.

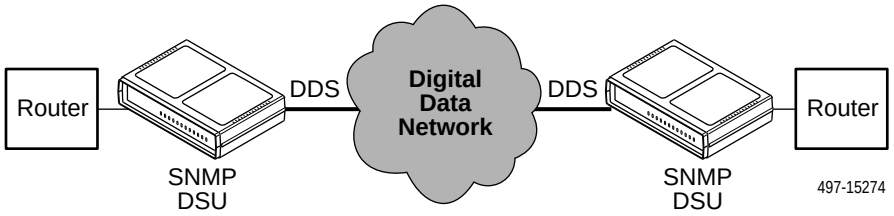
Supported Link-Layer Protocols

The DSU supports two link-layer protocols for connection to an external SNMP manager or network device:

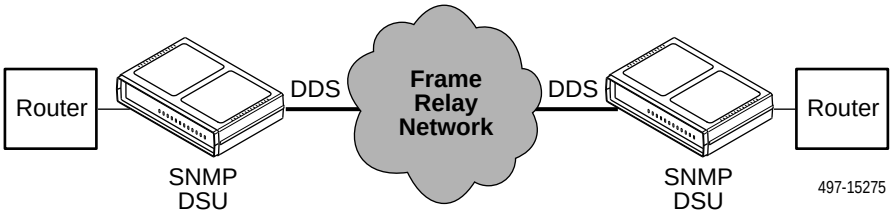
- Point-to-Point Protocol (PPP)
- Serial Line Internet Protocol (SLIP)

Typical SNMP DSU Configurations

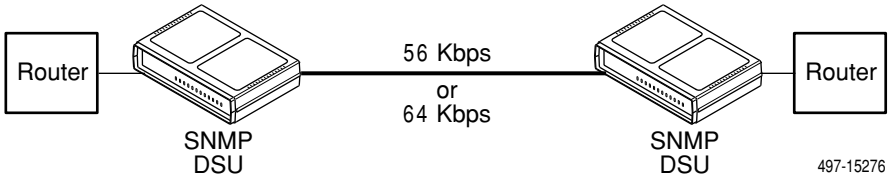
The following illustration shows a typical LAN/WAN interconnection application for the DSU. The routers connected to the DSU at each location provide the LAN interconnection.



The SNMP DSU can also be used in a frame relay network.



Two SNMP DSUs can be connected back-to-back to act as Local Area Data Sets. Table 3 in the *Model 7610 DSU Startup Instructions* shows the maximum distances for LADS applications.



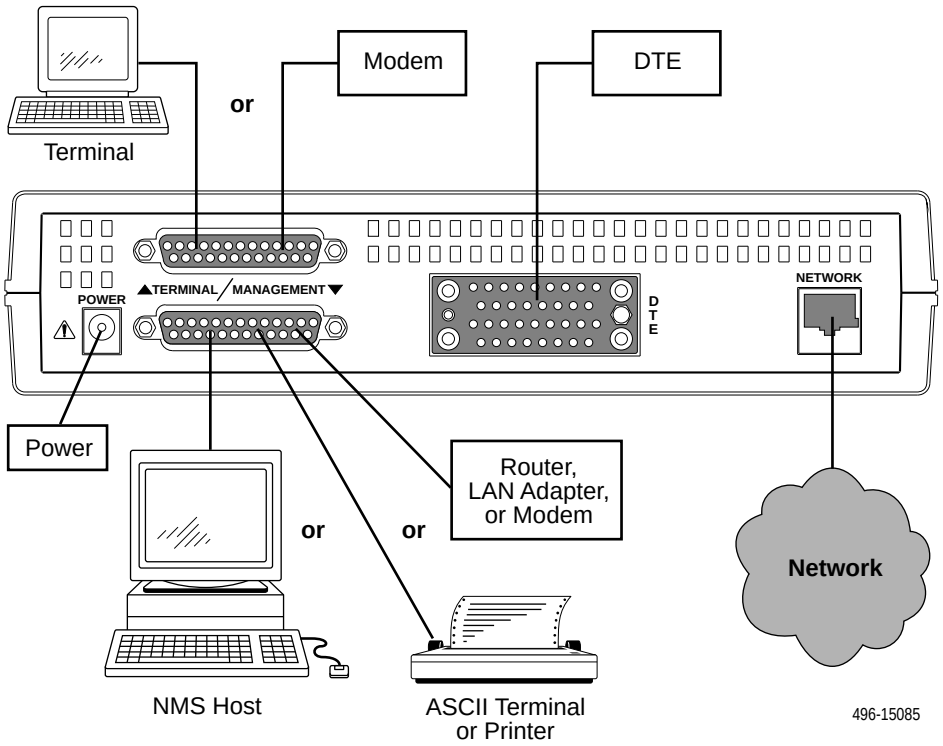
User Interface Types

There are three types of user interfaces for the SNMP DSU:

- Menu-driven async terminal interface screens (see *Using the ATI*, Chapter 2).
- SNMP NMS Access – Refer to the *SNMP DSU Features* section. Provides the capability to access the DSU via an SNMP management system connected to the Management port or remotely through the in-band management channel (IMC) connection. Refer to *IP Addressing*, Chapter 5.
- Front panel LED status indicators. Refer to *Monitoring the DSU*, Chapter 6.

Rear Panel Interface Connections

The following illustration shows the physical interfaces of the DSU. Information about the installation of the DSU is contained in the *Model 7610 DSU Startup Instructions*.



Using the ATI

2

Accessing the ATI

You can communicate with the Asynchronous Terminal Interface (ATI) using one of the following methods:

- Direct connection through the Terminal port.
- Dialing in through an external modem to the Terminal port.
- Telnet session through the Management port (locally or via an external modem).
- Telnet session through the In-band Management Channel (IMC).

NOTE:

Only one asynchronous user interface 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 (see Terminal Port Options, Table A-4).

The user interface is blank until activated. Press Return to activate the user interface. Security can limit ATI access several ways. To setup security or a login ID, refer to *Security*, Chapter 4.

Connecting to the Terminal Port

Verify that the settings of the device that you connect to the Terminal port match these factory-loaded option default settings:

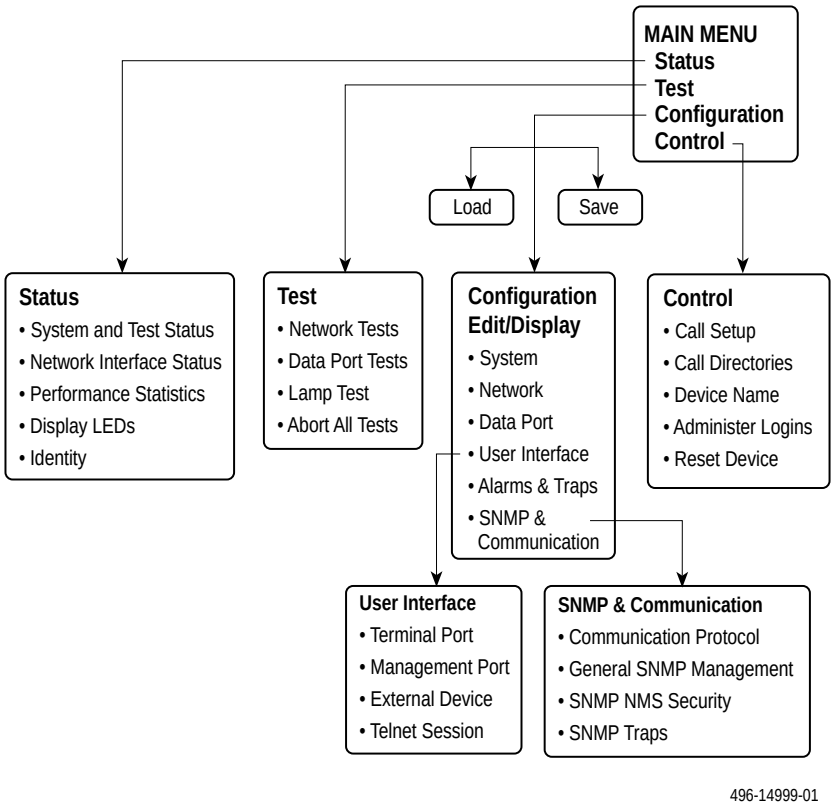
- Data rate set to 9.6 kbps.
- Character length set to 8.
- Parity set to None.
- Stop Bits set to 1.

To change the Terminal Port settings, refer to Terminal Port Options, Table A-4.

Main Menu

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

Select . . .	To . . .
Status	View diagnostic tests, network status of interfaces, statistics, LEDs, and DSU identity information.
Test	Select and cancel tests for the DSU's interfaces.
Configuration	Display and edit the configuration options.
Control	Control the user interface for call setup, device naming, and login administration, or to initiate a power-up reset of the DSU.



Screen Format Types

Three types of screen formats are available on the ATI.

Use the screen format . . .	To . . .
Menu selection	Display a list of available functions for user selection.
Input	Add or change information on a screen. Input or edit fields that have an Underline in the field value or selection. See *Screen Work Areas*.
Display	Display configuration information and results from performance and DSU-specific tests. Display-only fields that have no underline in the field value.

What Affects Screen Displays

What appears on the screens depends on the:

- **Current configuration** – How your DSU 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.

Screen Work Areas

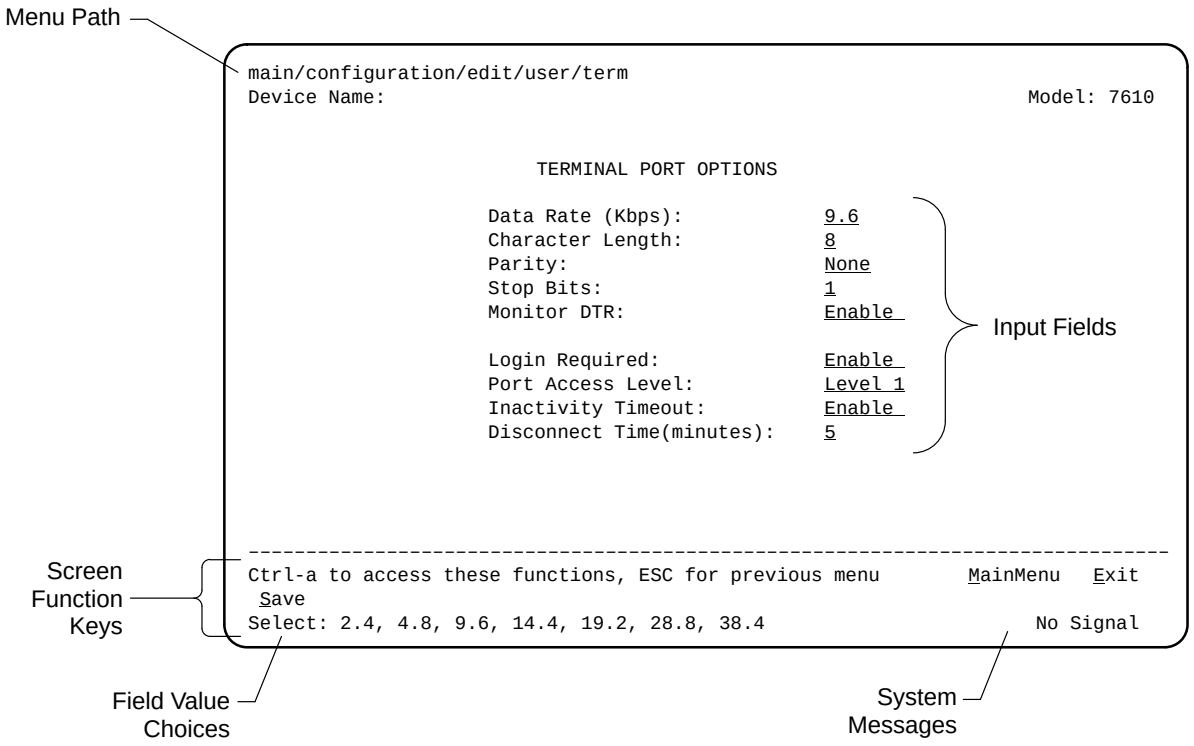
There are two user work areas:

- **Screen area** – Provides the menu path, access level, menus, and input fields above the dotted line. Refer to *Entering Device and System Information* in Chapter 3.

  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 → Edit → User Interface → Terminal Port

- **Screen function key area** – Provides functions available below the dotted line based upon screen selection and access level. Refer to the *Switching Between Screen Work Areas* section.



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.

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

To make a menu or field selection:

▶ Procedure

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 Return. 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, using the DSU's character matching feature.
- 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.

For the screen function . . .	Select . . .	And press Return to . . .
MainMenu	M or m	Return to the Main Menu screen.
Exit	E or e	Terminate the async terminal session.
New	N or n	Enter new data.
Modify	O or o	Modify existing data.
Delete	L or l	Delete data.
Save	S or s	Save information.
Refresh	R or r	Update screen with current information.
Clear	C or c	Clear status messages for one-time events on the System and Test Status screen.
ClrStats	C or c	Clear statistics and refresh the Network Performance Statistics screen.
PgUp	U or u	Display the previous page.
PgDn	D or d	Display the next page.
ResetMon	R or r	Reset an active Monitor 511 test counter to zero.

Switching Between Screen Work Areas

Selecting Ctrl-a allows you to switch between the two screen work areas to perform all screen functions. To access the screen function area below the dotted line:

▶ Procedure

1. Press Ctrl-a to switch from the screen area to the screen function key area below the dotted line. The available selections for the first input field appear on the last line as shown below.
2. Select either the function's designated (underlined) character or press the tab key until you reach the desired function key.

   Example:
   To leave the current screen, enter e or E (Exit).
3. Press Return. The function is performed.
4. To return to the screen area above the dotted line, press Ctrl-a again.

```
main/configuration/edit/user/mgmt
Device Name:                                                    Model: 7610


                        MANAGEMENT PORT OPTIONS

                    Port Use:                     Net Link
                    Port Type:                    Synchronous
                    Clock Source:                 Internal
                    Data Rate(Kbps):              9.6
                    Routing Information Protocol: None



--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu   Exit
 Save
Select: None, Net Link, Alarms.
```

Ending a Session

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

▶ Procedure

1. Press Ctrl-a to go to the screen function key area below the dotted line.
2. Save changes if you have altered your configuration.
3. Select Exit and press Return. The Main Menu appears.

Customizing the SNMP DSU

3

Entering Device and System Information

Use the Device Name screen to input DSU device and SNMP system entries. To access the Device Name screen, follow this menu selection sequence:

Main Menu → Control → Device Name

```
main/control/device name
Device Name:                                                    Model: 7610


                                DEVICE NAME

    Device Name:     NE815378 ___________________                Clear
    System Name:     lllQJ98-001_____________________________    Clear
    System Location: Bldg. A412, 2nd Floor, Left cabinet_______  Clear
    System Contact:  Joe Smith 800-555-5555 pager 888-555-5555   Clear




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

Any printable ASCII characters are valid entries for all the Device Name screen inputs. Refer to the *ASCII Characters* section in Appendix A. The Device Name field is alphanumeric and provides for an input of 20 characters. The Device Name entry appears on all ATI screens. The input on this screen is displayed on the Identity screen. Refer to the *Identity Information* section.

System Fields

The three System entry fields are alphanumeric and provide 127 characters for each field. The System entries appear on the Identity display as shown in the next section. 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

Press Ctrl-a to switch to the screen function key area below the dotted line. Select Save and press Return. When Save is complete, Command Complete appears at the bottom of the screen.

Identity Information

The Identity screen provides identification information about the DSU. To view information on the three System entries beyond the 40 characters on the screen, place the cursor on the first or last character and press the left or right arrow.

To access the Identity screen, follow this menu selection sequence:

Main Menu → *Status* → *Identity*

```
main/status/identity
Device Name: NE815378                                          Model: 7610

                                IDENTITY

    System Name:     lllQJ98-001
    System Location: Bldg. A412, 2nd Floor, Left cabinet
    System Contact:  Joe Smith 800-555-5555 pager 888-555-5555
                Serial Number:       1234567
                Model Number:        7610-A1-201
                Software Revision:   01.00.00
                Hardware Revision:   2048-80A


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

Configuring the DSU

Configuration option settings determine how the DSU operates. Use the DSU's Configuration branch to display or change configuration option settings.

Configuration Option Areas

The DSU is shipped with factory settings in the Default Factory configuration option area. You can find default information by:

- Referring to *Configuration Option Tables*, Appendix A, or *Worksheets*, Appendix B.
- Accessing the Configuration branch of the DSU menu.

The DSU offers four sets of configuration option settings located in the following areas. The first three sets match the Default Factory Configuration options set until modified and saved by the user.

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

Configuration Option Area	Configuration Option Set
Current Configuration	The DSU's active set of configuration options.
Customer Configuration 1	Use to set up and store a set for future use.
Customer Configuration 2	Use to set up and store a second set for future use.
Default Factory Configuration	A read-only configuration area containing the factory default configuration options.

Accessing and Displaying Configuration Options

To display the configuration options, you must first copy one configuration option set into the edit area.

▶ Procedure

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

   Main Menu → Configuration → Load Configuration From

2. Select one of the four configuration option areas listed. Press Return. The selected configuration option set is loaded and the Configuration Edit/Display menu screen appears.

   No configuration edits are allowed when the effective access level is 2 or 3. Configuration is read-only and allows viewing only of configuration option settings. If the effective access level is not an access level of 1:

   — The last line of the Load Configuration From screen reads:

   Access Level is *n*, Configuration is read-only

   — The Save prompt will not appear on any screens.

Refer to *Security*, Chapter 4.

Saving Configuration Options

When changes are made to the configuration options, the changes must be saved to take effect. The Save key and Save Configuration To screen appear when the user has an effective access level of 1. All other effective access levels have read-only permission.

To save configuration options changes:

▶ Procedure

1. Press Ctrl-a to switch to the screen function key area below the dotted line.
2. Select Save and press Return. The Save Configuration To screen appears.
3. Select one of the three configuration option areas on the screen and press Return. When Save is complete, Command Complete appears in the message area at the bottom of the screen.

NOTE:

When Exit is selected before Save, a Save Configuration screen appears requiring a Yes or No response.

If you select . . .	Then . . .
Yes	The Save Configuration To screen appears.
No	The Main Menu appears and changes are not saved.

Establishing Call Setup

From the Control menu, Call Setup is available for the Management port when connected to an external device, such as a modem or an X.25 PAD. Before completing the Call Setup screen entries, the phone numbers need to be entered on the Call Directories screen.

Call Directories Screen

Use the Call Directories screen to enter or change the phone numbers used to:

- Send out an ASCII alarm message to an ASCII terminal or printer.
- Send out an SNMP trap message.
- Connect to an NMS for dial-in management.

To access the Call Directories screen, follow this menu selection sequence:

Main Menu → Control → Call Directories

```
main/control/directories
Device Name:                                                    Model: 7610

                                CALL DIRECTORIES

    Primary Directory:

    Phone Number: xxxxxxx                                       Clear

    Alternate Directory:

    Phone Number: xxxxxxx                                       Clear


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

The Phone Number fields allow 40 characters. For valid Call Directory entries, refer to Table 3-1.

After entering or changing a phone number, press Ctrl-a to go to the function key area below the dotted line. Select Save and press Return.

Table 3-1. Call Directory Phone Number Entries

Characters	Use
B	Blind dialing; do not wait for dial tone
P	Pulse dialing unless preceded by a B
T	Tone dialing unless preceded by a B
W	Wait for dial tone before dialing
, (comma)	Two-second pause; do not use in dial string
< > (space)	Readability; character ignored during automatic dial-out
– (hyphen)	Readability; character ignored during automatic dial-out
ASCII Characters	Refer to Appendix A

Call Setup Screen

Use the Call Setup screen to:

- Initiate or disconnect an active call with an external device. External Device Commands option must be set to AT or Other (not to Disable). Refer to External Device Options, Table A-6.
- Display the phone number entered on the Call Directories screen.

To access the Call Setup screen, follow this menu selection sequence:

Main Menu → Control → Call Setup

```
main/control/setup
Device Name:                                                    Model: 7610

                                  CALL SETUP

        Directory: Primary
        Phone Number: xxxxxxx
        Dial
        Disconnect




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

Select: Primary, Alternate
```

After completing call setup, the Management port can be used to send out ASCII alarms and SNMP traps. The Alarm & Trap Dial-Out option must be enabled. Refer to Alarms & Traps Options, Table A-8.

Security

4

Security Overview

The DSU provides several methods of security by limiting user access to the ATI through option settings. Refer to the *ATI Access* section.

- Enable the Login Required option to require a Login ID for the:
  - Terminal Port
  - Telnet Session via the IP interfaces (the Management port or the IMC)
- Limit the access:
  - Port Access Level option of 1, 2, or 3 for the Terminal port
  - Session Access Level option of 1, 2 or 3 for the Telnet Session
- Disable the access:
  - Telnet Session option
  - Management Port Use option
  - In-Band Management Channel Rate (bps) option for the IMC
  - Dial-In Access option for an External Device

Refer to Effective Access Levels, Table 4-1.

SNMP security is handled through Community Names with access levels and IP address validation. Refer to the *Controlling SNMP Access* section.

Creating a Login

Logins apply to Terminal port and Telnet access to the ATI. Six login ID/password combinations are available. Each Login ID and Password must be unique and include an access level.

For additional information regarding the ATI access using the Login Required option, refer to the *ATI Access* section.

▶ Procedure

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

   Main Menu → Control → Administer Logins

2. Press Ctrl-a to switch to the screen function key area below the dotted line.
3. Select New and press Return.
4. Create the login by entering the following fields. For valid entries in the first two fields, refer to the *ASCII Characters* section of Appendix A.

On the Administer Logins screen, for the . . .	Enter . . .
Login ID	1 to 10 ASCII printable characters
Password	1 to 10 ASCII printable characters
Access Level	Level 1, Level 2, or Level 3

NOTE:

Assign at least one Level 1 Access Level. Full access is necessary to make configuration option changes and administer logins. If there is no effective access level 1, refer to the *Device Reset* section of Chapter 7.

5. Press Ctrl-a to switch to the screen function key area below the dotted line. Select Save and press Return.
6. When Save is complete, Command Complete appears at the bottom of the screen. The cursor is repositioned at the Login ID field, ready for another entry.

Deleting a Login

▶ Procedure

1. To delete a login record, follow this menu selection sequence:

   Main Menu → Control → Administer Logins

2. Press Ctrl-a to switch to the screen function key area below the dotted line.
3. Select PgUp or PgDn and press Return to page through login pages/records until you find the one to be deleted.
4. Once the correct record is displayed, select DeLete and press Return.
5. To complete the delete action, select Save and press Return.

   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.

ATI Access

Access to the ATI is available through either the Terminal port or a Telnet session.

Access to the ATI through the Terminal port can be limited. Refer to Terminal Port Options, Table A-4, to:

- Enable Login Required.
- Assign a Port Access Level of 1, 2, or 3.

The ATI can be accessed remotely through a Telnet Session via either the Management port or the IMC. The DSU provides several methods for limiting access to the ATI through a Telnet session.

- Refer to Telnet Session Options, Table A-7, to:
  - — Enable Login Required.
  - — Assign a Telnet Session Access Level of 1, 2, or 3.
  - — Disable Telnet access completely.
- To prevent the Management port and IMC from supporting a Telnet session:
  - — Set the Port Use option to None or Alarms. Refer to Management Port Options, Table A-5.
  - — Disable the IMC using the In-Band Management Channel Rate (bps) option in Table A-2.

Effective Access Level

The ATI effective access level is the more restrictive between the Port/Session access level and the Access level associated with the Login ID. For example, if a login ID is created with an Access Level 1 and the Terminal Port is set for a Port Access Level of 2, the effective access level to the ATI is 2.

Table 4-1. Effective Access Levels

ATI Access to Menu Functions	Effective Access Level 1	Effective Access Level 2	Effective Access Level 3
Status	Read-Only	Read-Only	Read-Only
Test	Full Access	Full Access	No Access
Configuration	Full Access	Read-Only	Read-Only
Control	Full Access	No Access	No Access

When user access to the ATI is attempted through the Terminal port or a Telnet session, the ATI response is based on the Login Required option and the availability of the ATI.

Table 4-2. ATI Access Conditions

If access to the ATI is through the . . .	Then . . .	What to do now?
Terminal port with Security disabled with the Login Required option set to Disable. (See Table A-4)	The Main Menu screen appears.	Select a menu option to begin your session.
Terminal port with Security enabled with the Login Required option set to Enable. (See Table A-4)	You are prompted for a login ID and password.	If Invalid Password appears, re-enter the password. After three tries with an invalid password, contact the system administrator.
	The Main Menu screen appears if the login ID is not configured yet.	Select a menu option to begin your session.
Terminal port and the ATI is already in use with a Telnet session	**User Interface Already In Use** message appears with the active user's IP address and Login ID.	Try again later. When the ATI is available, the message **User Interface Idle** appears.
Telnet session and the ATI is currently in use	**Connection Refused** message appears. The DSU allows only one connection at a time.	Try again later.

Controlling SNMP Access

There are three methods for limiting SNMP access.

- Disable the SNMP management option.
- Assign SNMP community names and access levels. The DSU supports SNMP Version 1, which provides limited security through the use of community names.
- Limiting SNMP access through validation of the IP address of each allowed SNMP manager.

Assigning SNMP Community Names and Access Levels

The DSU can be managed by an SNMP manager supporting the SNMP protocol. 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 & Communication → General SNMP Management

Refer to General SNMP Management Options, Table A-10, to:

- Enable SNMP Management.
- Assign the SNMP community names of the SNMP Managers that are allowed to access the DSU'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 DSU 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 → Load Configuration From → Edit → SNMP & Communication → SNMP NMS Security Options

Refer to SNMP NMS Security Options, Table A-11. The SNMP access can be limited by:

- Enabling NMS IP address validation to perform validation checks on the IP address of an SNMP management system attempting to access the DSU.
- Specifying read or read-write access for each NMS authorized to access the unit.

IP Addressing

5

Selecting an IP Addressing Scheme

You can select from many IP addressing schemes to provide SNMP NMS connectivity. Review the following information in preparation for selecting an IP addressing scheme.

- Assign IP addresses to:
  - — The Management port
  - — The IMC

  Refer to the *IP Addressing Scheme Examples* section.
- When the Routing Information Protocol (RIP) option is set to Proprietary, IP routing information is automatically passed between interconnected DSUs from the network side. Refer to Management Port Options, Table A-5.

  However, verify that a route to the subnet(s) is set in the NMS's or local router's routing table. This equipment will not automatically receive routing information due to the proprietary protocol.

  The gateway to subnet(s) is through the DSU connected to:
  - — The LAN using a LAN adapter, or
  - — A router, terminal server, or NMS via PPP or SLIP link-layer protocols
- Each DSU's routing table supports a maximum of 20 routes, even though a single route is all that is needed to reach every device on a subnet.
- Set a default route only for devices directly connected to the DSU's Management port.
- Any legal host address is allowed for a given subnet; the address choice within the subnet is completely arbitrary.

IP Addressing Scheme Examples

Management of IP addressing is based upon individual IP addresses assigned to each interface. The IP interfaces for the unit are the:

- Management port: Set the Port Use option to Net Link; see Management Port Options, Table A-5.
- IMC: Set the In-Band Management Channel Rate (bps) to 1600, 4000, or 8000 bps; see Network Interface Options, Table A-2.

NOTE:

For IP addressing, involve your Information Systems (IS) department since the department decides on the IP addressing scheme used for your organization.

The following illustrations and examples apply to IP management traffic only. The subnet mask shown for these examples is 255.255.255.000.

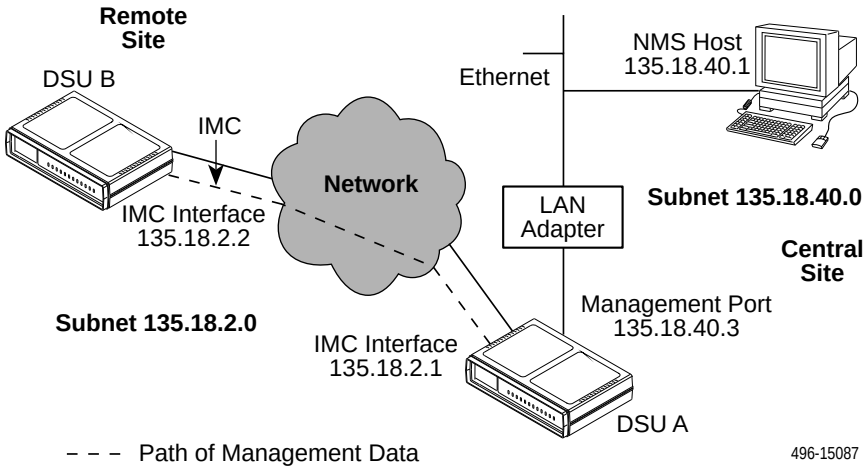
IMC Connection – Same Subnet

In this example, DSU A is connected to:

- The NMS, at the central site, via a LAN adapter
- A remote unit, DSU B, through the proprietary IMC

NOTE:

Interconnected DSUs will automatically pass routing information between each other using a proprietary protocol. However, a static route to subnet 135.18.2.0 must be set in the routing table of the NMS Host.

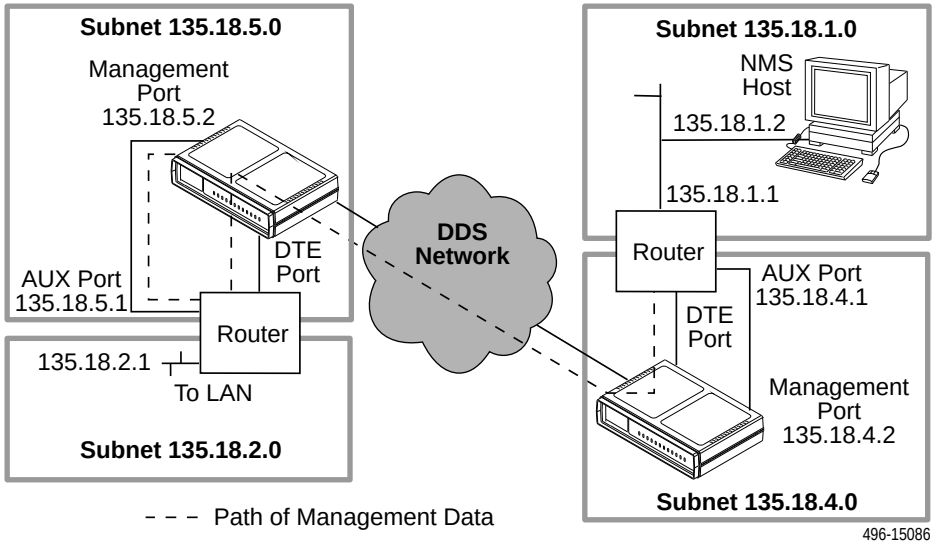


Using Routers to Route DSU Management Data

In this example, the DSUs:

- Receive their management data through the Management port connection to the AUX port of the router.
- Do not route the data among themselves. Routers route management data for the connected DSUs using the management data path between the routers.

The illustration shows each DSU with its own subnet. This subnet is independent of the subnet on the LAN, which is supported by the local router. This enables the router to distinguish the data destined for the DSU from the data for the LAN.



Assigning IP Addresses and Subnet Masks

Once you select an IP scheme, assign an address(es) to the DSU.

If using . . .	Then . . .
The Management port as a management interface	Assign the Management port IP address and subnet mask. Refer to Communication Protocol Options, Table A-9.
An external modem connected to the Management port, and you want to configure an alternate IP address and subnet mask for dialing out traps using the alternate alarm directory	Enter the alternate Management port IP address and subnet mask. Refer to Communication Protocol Options, Table A-9.
The IMC	Assign the IP address and subnet mask. Refer to Network Interface Options, Table A-2.

The SNMP NMS Security Options screen provides options to perform security checking on the IP address of the SNMP management system attempting to communicate to the DSU. Refer to SNMP NMS Security Options, Table A-11.

Choosing a Default Network Destination

You can route an SNMP or Telnet session to a default network destination. To configure a Default Network Destination, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → SNMP & Communication → Communication Protocol

Refer to Communication Protocol Options, Table A-9.

Monitoring the DSU

6

What to Monitor

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

- LEDs on the ATI Status screen or the DSU's front panel
- Unit Status screen on the ATI
- Highest priority Health and Status message displays on the right on the last line of all screens.
- Network Interface Status screen on the ATI
- Network Performance Statistics screen on the ATI
- NMS via SNMP MIB objects

Refer to *MIB Descriptions*, Appendix C, for the SNMP MIBs supported by the DSU.

DSU LEDs

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

The 12 LEDs are organized in three groups:

- **System** LEDs display the status of the unit
- **Network** LEDs provide the status of the network interface
- **Port** LEDs display the activity on the user data (DTE) port

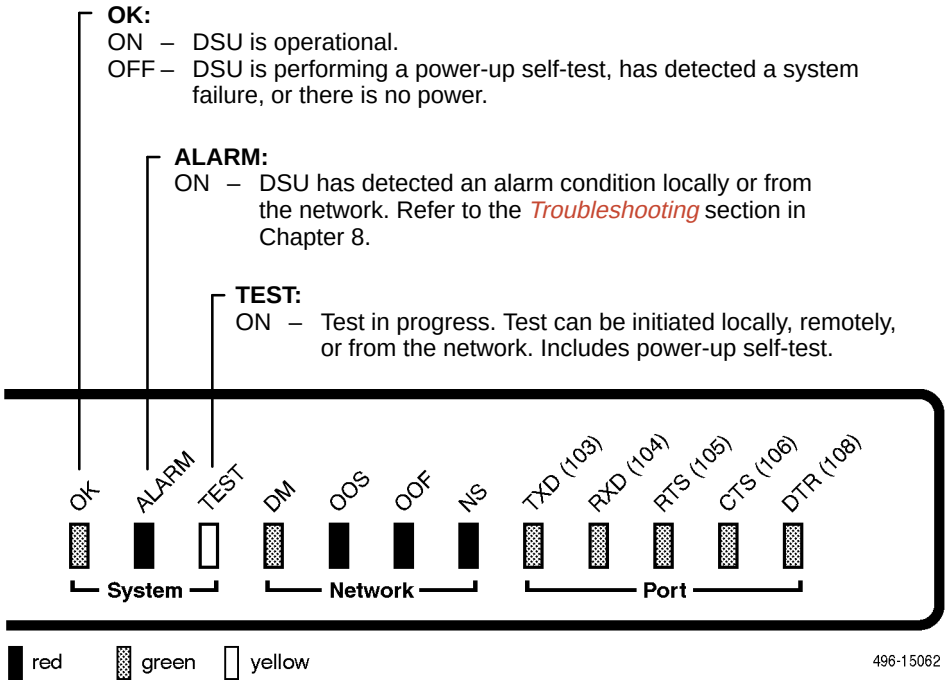
To view the LED status screen, follow this menu selection sequence:

Main Menu → Status → Display LEDs

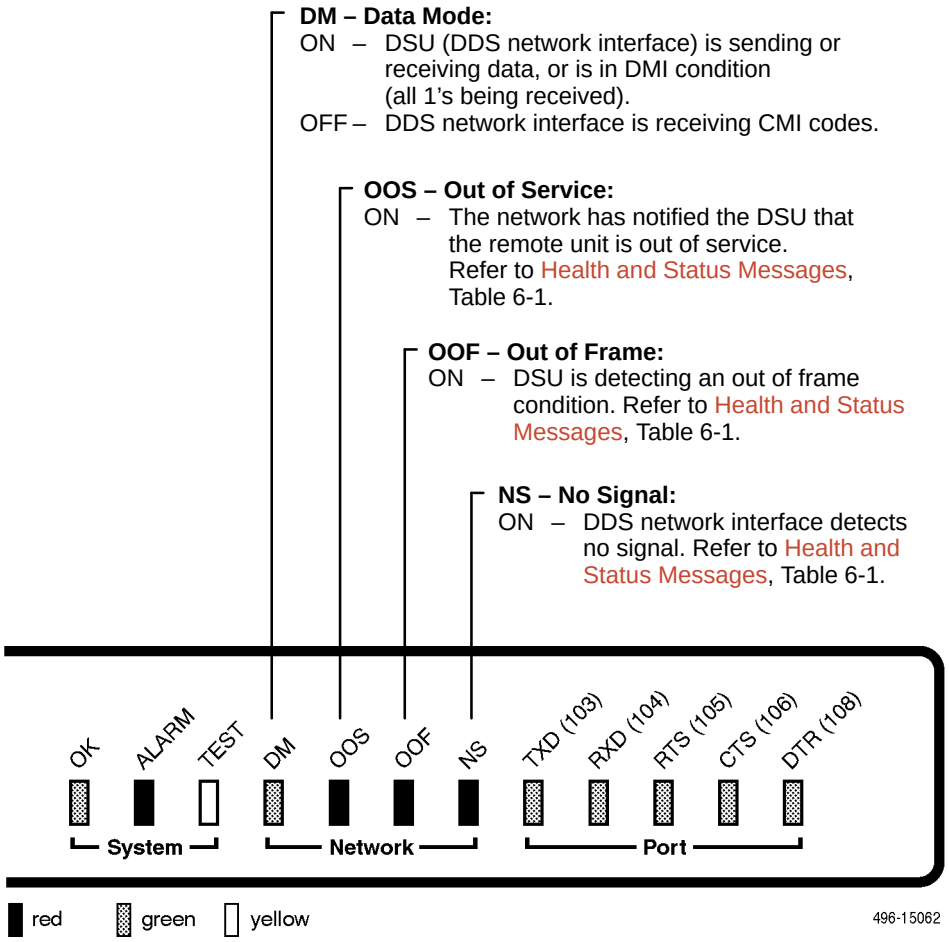
```
main/status/leds
Device Name:                                                    Model: 7610

                              DISPLAY LEDS

        SYSTEM                    NETWORK                        DTE

    OK   ALARM  TEST        DM  OOS  OOF  NS        TXD   RXD  RTS  CTS  DTR
                                                      |     |
                                                  blinking  blinking

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

When viewed via the ATI, the status display screen is updated approximately every 5 seconds. Use Refresh to obtain a current status of all LEDs.

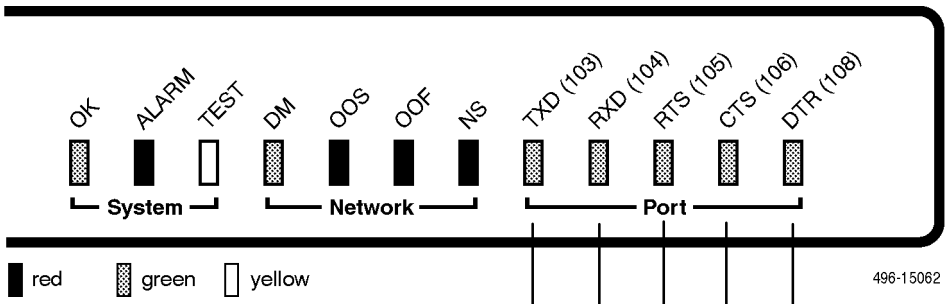
System LEDs



Network LEDs



Port LEDs



TXD – Transmitted Data:
ON – Receiving all 0s from the DTE.
OFF – Receiving all 1s from the DTE.
Blinking – User data is being transferred.

RXD – Received Data:
ON – Sending all 0s to the DTE.
OFF – Sending all 1s to the DTE.
Blinking – User data is being transferred.

RTS – Request to Send:
ON – DTE is activating a control signal to indicate readiness to transmit data.

CTS – Clear to Send:
ON – DSU is activating a control signal to indicate to the DTE that it can start sending data.

DTR – Data Terminal Ready:
ON – DTE is activating a control signal to indicate readiness for operation.

Unit Status

Status is a branch of the ATI main menu. From Status, the System and Test Status screen is available and has three sections:

- **Health and Status** – Displays messages in priority order (highest to lowest). Refer to Health and Status Messages, Table 6-1.
- **Self-Test Results** – Results of the Diagnostic test run on the device itself. Refer to Self-Test Results Messages, Table 6-2.
- **Test Status** – Currently active tests. Refer to Test Status Messages, Table 7-1.

Viewing Health and Status

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

Main Menu → *Status* → *System and Test 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. The messages are listed from high to low priority in Table 6-1.

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

Message	What Message Indicates	What To Do
Cross Pair Detection	The DDS Receive (RX) and Transmit (TX) pairs are crossed on the network interface. Alarm LED is on.	Reverse the RX and TX pair at the punchdown block or other termination point.
No Signal *hhh:mm:ss*[1]	No signal is being received. Local DSU network problem. The Alarm and NS LEDs are on and Network Performance Statistics are active.	1. Verify that the network cable is securely attached at both ends. 2. Contact network provider.
Out of Service *hhh:mm:ss*[1]	DSU is receiving out of service code from the network for the remote unit. The Alarm and OOS LEDs are on and Network Performance Statistics are active.	1. Verify that the remote site is in service. 2. Contact network provider.
[1] *hhh:mm:ss* indicates the amount of time the condition has existed in hours, minutes, and seconds. When the maximum time has been exceeded, 255:59:59+ appears.		

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

Message	What Message Indicates	What To Do
Out of Frame *hhh:mm:ss*[1]	DSU is detecting an out of frame condition, associated with: ■ Receiving out of frame code from the network. ■ DSU detecting out of frame errors with 64 kbps CC data rate. ■ DSU unable to synchronize local receiver circuit with line signal.	1. Verify that the line rate matches the configured rate. 2. Contact network provider.
Excessive BPVs *hhh:mm:ss*[1]	Data rates do not match or network trouble causing bipolar violations. Alarm LED is on and Network Performance Statistics are active.	1. Verify that the network cable is securely attached at both ends. 2. Contact network provider if problem persists.
In-Band Fram Err *hhh:mm:ss*[1]	The IMC communication between the local and remote DSU is not working.	1. Verify that the remote unit has IMC set at the same rate. 2. Contact network provider if problem persists.
User Data Port DTR Off	The DTE is not ready to transmit or receive data. This message will not appear unless Monitor DTR is enabled.	Check on the DTE status. Verify that the DTE is powered up and asserting DTR.
Net Mgmt Link Down	Communications between the DSU and an NMS are not possible and the: ■ Management Port Use is set to Net Link and/or ■ IMC is enabled.	1. Check the devices in the management path data and the status of the NMS. 2. Try to access the unit remotely.
Device Fail *yyyyyyyy*	An internal error has been detected by the operating software. *yyyyyyyy* indicates the 8-digit hexadecimal failure code.	1. Provide the 8-digit failure code shown (*yyyyyyyy*) to your service representative. 2. Reset the DSU to clear the condition and message.
DSU Operational	DSU is functioning properly and there are no status messages to display.	No action needed.

[1] *hhh:mm:ss* indicates the amount of time the condition has existed in hours, minutes, and seconds. When the maximum time has been exceeded, 255:59:59+ appears.

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 6-2. Self-Test Results Messages

Message	What Message Indicates	What To Do
Device Fail	One or more of the DSU's integrated circuit chips has failed device-level testing.	1. Reset the DSU and try again. 2. Call your service representative for assistance if the message reappears.
Memory Fail	DSU failed memory verification.	
Passed	The DSU has been plugged in or reset and has passed the diagnostic test. There are no other status messages.	No action needed.

Network Interface Status

The network interface status fields are read-only:

- Line Rate (Kbps). If the DSU is connected to an operating line and the Line Rate (Kbps) shows Autobaud and does not change to a line rate within about 25 seconds, Line Rate (Kbps) may have to be reconfigured manually. Refer to System Options, Table A-1.
- Loop Loss (dB). The loop loss is the loss of signal strength of the receive line signal from the local loop.

To view the Network Interface Status, follow this menu selection sequence:

Main Menu → *Status* → *Network Interface Status*

Table 6-3. Network Interface Status Screen Contents

Field	Status	What the Status Indicates
Line Rate (Kbps)	56 Kbps 64 CC 64 LADS Autobaud	Line rate on the network interface. Autobaud indicates the DSU is trying to determine the network line rate. This should be a temporary condition.
	No Signal	No signal can be detected over the network interface.
Loop Loss (dB)	0 to –65 dB	Amount of loop loss – loss of signal strength of the receive line signal from the local loop, measured in decibels.
	Inoperative	The line may be disconnected.

Network Performance Statistics

Performance statistics for the network interface are available to:

- Monitor the current status of the network operations.
- View the DSU's performance statistics, which:
  - — Assist you in determining the duration of specific conditions.
  - — Provide a historical context for problem detection and analysis.

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

Main Menu → *Status* → *Performance Statistics*

```
main/status/performance
Device Name:                                                    Model: 7610


                    NETWORK PERFORMANCE STATISTICS

                No Signal Count:        101920     26:33:08
                Out of Service Count:        0      0:00:00
                Out of Frame Count:        621      8:53:49
                Excessive BPV Count:     99830    144:28:11
                Invalid BPV Count:       87409


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

All counts show the number of occurrences since the last reset of the counters. Invalid BPV is a raw count of the number of invalid Bipolar Violations. In the last column, *hhh:mm:ss* indicates the amount of time the condition has existed in hours, minutes, and seconds. When the maximum time has been exceeded, 255:59:59+ appears.

The screen appears with the cursor in the function area below the dotted line. To update the performance statistics, select Refresh and press Return.

Select ClrStats and press Return to clear all statistics and refresh the screen. ClrStats is not available for an Access level of 3.

Testing

7

Detecting Problems

The DSU can detect and report problem conditions and perform diagnostic tests. The DSU offers a number of indicators to alert you to possible problems:

- LEDs – Refer to the *DSU LEDs* section in Chapter 6.
- SNMP Traps – For information on traps, refer to the *Configuring SNMP Traps* section in Chapter 8.
- Health and status messages and network performance statistics. Refer to *Monitoring the DSU*, Chapter 6.
- Alarm Condition Indications.

The following table shows the available indicators of alarm conditions on the network interface and the User Data port.

Alarm Condition	SNMP Trap	ATI Status Screen	ASCII Alarm (if configured)	Alarm LED	Specific LED
Crossed Pairs	Y[1]	Y	Y	Y	N
No Signal (NS)	Y[1]	Y	Y	Y	Y
Out of Service (OOS)	Y[1]	Y	Y	Y	Y
Out of Frame (OOF)	Y[1]	Y	Y	Y	Y
Excessive Bipolar Violations (BPV)	Y[1]	Y	Y	Y	N
Inband Framing Error	N	Y	Y	Y	N
DTR Off	Y[1]	Y	N	N	Y
[1] Link Up/Link Down Trap					

To configure ASCII Alarms, use the Alarms & Traps options screen. Refer to Alarms & Traps Options, Table A-8. For additional information regarding ASCII alarm generation, refer to the *Alarm Messages* section of Chapter 8.

Tests Available

From the Test menu, you can run network tests, data port tests, and a lamp test for the front panel LEDs. Loopbacks can be initiated locally and remotely. Refer to Loopbacks, Table 7-2.

The Test menu is limited to users with an access level of 1 or 2. To access the Test menu, follow this menu selection sequence:

Main Menu → Test

Network tests require the participation of your network service provider.

The DSU supports physical-level tests independently on a per-interface basis.

- The CSU and DSU loopbacks and 511 test pattern send/monitor are supported on the network interface.
- The Local Loopback and 511 test pattern send/monitor are supported on the DTE port.

Network Tests

To access the Network Tests screen, follow this menu selection sequence:

Main Menu → Test → Network Tests

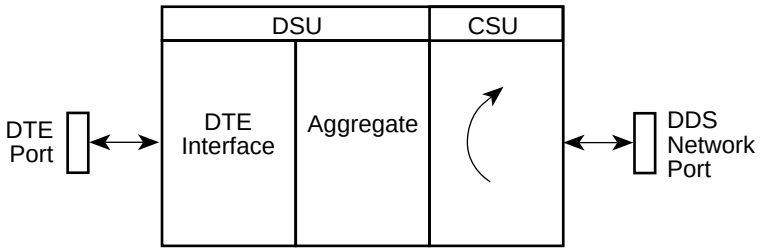
```
main/test/network
Device Name:                                                  Model: 7610

                            NETWORK TESTS

    Test            Command   Status          Result

    CSU Loopback:   Start     Inactive          0:00:00
    DSU Loopback:   Start     Inactive          0:00:00

    Send V.54 Up:   Send      Sending
    Send V.54 Down: Send      Inactive

    Send 511:       Start     Inactive          0:00:00
    Monitor 511:    Stop      Active          125:08:48   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 by pressing Enter. The Result column displays the test duration since the last device reset. When the Monitor 511 test is active, ResetMon is available to reset the error counter to zero.

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

CSU or External Network Loopback

CSU loopback is an external loopback that is located as close as possible to the network interface. An active CSU loopback disrupts IP data going over the IMC.

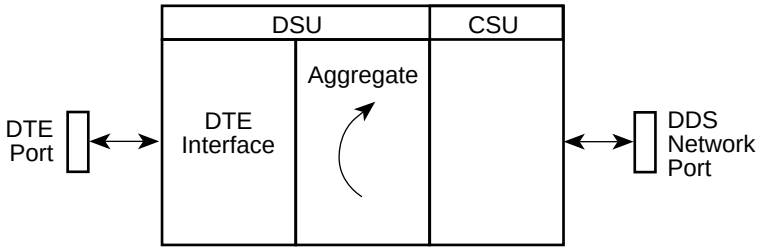


CSU Loopback 496-15144

DSU or Internal Network Loopback

DSU loopback is an internal loopback that is located as close as possible to the customer interface serving the DTE.

An active DSU loopback initiated from the network disrupts IP data going over the IMC. However, this test is not disruptive when initiated by the user (via ATI) or by the NMS.



DSU Loopback 496-15160

Send V.54 Up/Down Sequences

The local DSU can send an ITU-T V.54 Up or Down sequence to request the activation or termination of a DSU (digital) loopback of a remote unit. This is the same as the DSU Loopback shown above except the test is activated remotely.

The DSU can send:

- In-band V.54 Up (activation) code to request a Remote DSU Loopback (V.54 Loop 2) at the remote DSU or
- In-band V.54 Down (deactivation) code to request the termination of a Remote DSU Loopback (V.54 Loop 2) at the remote DSU

Refer to the *Network Tests* section for an example of the Network Tests screen. Select Send. Sending appears in the Status column followed (after 3 seconds) by Command Complete at the bottom of the screen.

511 Test Pattern for the Network

This test sends or monitors the 511 test pattern over the network interface.

The Monitor 511 test also provides an error counter that can be reset. Refer to the *Network Tests* section for an example of the Network Tests screen.

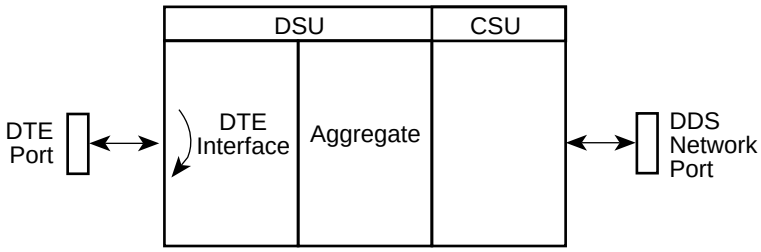
Data Port Tests

For an example of the fields on a test menu screen, refer to the *Network Tests* section. To access the Data Port Tests screen, follow this menu selection sequence:

Main Menu → Test → Data Port Tests

Local Loopback

Local Loopback loops the user data back to the DTE. This loopback is located as close as possible to the User Data Port (DTE) interface.



Local Loopback 496-15145

511 Test Pattern for the DTE

This test sends or monitors a 511 test pattern over the User Data Port interface.

The 511 monitor expects the external equipment to provide the clock for the 511 pattern on the interchange circuit CT113 – Transmit Signal Element Timing – DTE Source (XTXC or TT) for timing the incoming pattern. Refer to the *V.35 User Data Port Connector* section of Appendix E.

Lamp Test

The DSU supports a Lamp test from the Test menu to determine whether all LEDs are lighting and functioning properly.

During the Lamp test, all LEDs blink simultaneously every second. When you stop the Lamp test, the LEDs are restored to their normal condition.

Ending an Active Test

A test initiated by the user can be ended by the user.

- 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. Refer to System Options, Table A-1.

  Test Timeout does not pertain to tests commanded by the:

  — Network, such as the network-initiated CSU and DSU Loopbacks.

  — DTE, such as the DTE-initiated Local Loopback.

- On each test screen is a command column. Pressing Return when the cursor is on the Start command stops the test.

- Use the Abort All Tests selection from the Test menu to stop all tests running on all interfaces, with the exception of network or DTE-initiated loopbacks. Command Complete appears when all tests on all interfaces have been terminated.

Test Status Messages

The Test Status Messages in Table 7-1 appear in the right-most column of the System and Test Status screen. For additional information on loopbacks, refer to Loopbacks, Table 7-2.

Table 7-1. Test Status Messages (1 of 2)

Test Status Message	Meaning
CSU Loopback Active	A CSU Loopback toward the network is currently active. Only applies to a test initiated by the user via the ATI or the NMS.
DSU Loopback Active	A DSU Loopback toward the network is currently active. Only applies to a test initiated by the user via the ATI or the NMS.
Lamp Test Active	The Lamp Test is active, causing the LEDs on the front panel to light.
Local Loopback Active	A local loopback toward the DTE is currently active.
Monitoring 511 on Network	DSU is monitoring a 511 test pattern on the network interface.
Monitoring 511 on Port	DSU is monitoring a 511 test pattern over the DTE port.
Network-init. CSU LB Active	A CSU Loopback initiated by the network is currently active.

Table 7-1. Test Status Messages (2 of 2)

Test Status Message	Meaning
Network-init. DSU LB Active	A DSU Loopback initiated by the network is currently active. ■ If the network service is 56 kbps, the network loopback is non-latching. A non-latching loopback ends when the network activation codes stop. ■ If the network service is 64 kbps CC, the network loopback is latching. This condition can only occur when the Network Interface option Network-initiated DSU Loopback (64K CC) is enabled. Refer to Network Interface Options, Table A-2.
No Test Active	Status message, indicating no local, remote, or network test in progress.
Sending 511 on Network	A 511 test pattern is being sent over the network interface.
Sending 511 on Port	A 511 test pattern is being sent over the DTE port.
V.54-initiated DSU LB Active	A DSU loopback is active that was initiated by the detection of a V.54 sequence originated by the remote unit. This condition can only occur when V.54 Initiated DSU Loopback is enabled. Refer to Network Interface Options, Table A-2.

Loopbacks

Loopbacks can be started from a variety of points in the network. Refer to Table 7-2 for further information.

Table 7-2. Loopbacks (1 of 2)

Loopback Type	Initiated By	Notes
Bilateral Loopback	■ ATI ■ NMS ■ Remote unit sending V.54 sequence	When enabled, running a DSU loopback also automatically starts a local loopback. Refer to Data Port Options, Table A-3, to enable.
CSU Loopback	■ ATI (Network tests) ■ NMS ■ DDS Network, by loop current reversal	When initiated by the network, CSU Loopback cannot be disabled by the user. When IMC is enabled, the aggregate data is looped back to the network.
DSU Loopback (Digital)	■ ATI ■ NMS	When IMC is enabled, only user data is looped back to the network. Refer to Data Port Options, Table A-3.
Local Loopback	■ ATI ■ DTE via CT141 ■ NMS	Control via CT141 can be disabled. Refer to Data Port Options, Table A-3.

Table 7-2. Loopbacks (2 of 2)

Loopback Type	Initiated By	Notes
Network-initiated 56 kbps DSU Loopback (Non-latching loopback)	■ DDS Network	When IMC is enabled, the aggregate data stream is looped back to the network. Cannot be disabled by user.
Network-initiated 64 kbps CC DSU Loopback (Latching loopback)	■ DDS Network	Includes optional data scrambling and uses 25-second timer to detect the network sequence. When IMC is enabled, the aggregate data stream is looped back to the network. Can be disabled by user.
Remote Digital Loopback	■ Remote unit sending V.54 sequence	Same as a DSU Loopback but initiated by a remote unit via V.54 sequence. When IMC is enabled, only user data is looped back to the network. Can be disabled locally. Refer to Network Interface Options, Table A-2.
V.54 Sequences to remote unit	■ ATI ■ NMS ■ DTE via CT140	Control via CT140 can be disabled. Refer to Data Port Options, Table A-3.

Device Reset

The DSU can be reset locally or remotely. From the Control menu, select Reset Device and press Return. The DSU reinitializes itself, performing a Device Self-Test. Refer to Self-Test Results Messages, Table 6-2.

Misconfiguring the DSU could make the user interface inaccessible, leaving it in a state where an ATI session cannot be started through the Terminal port or via a Telnet session. If this occurs, DSU connectivity can be restored with a terminal that is directly connected and set for Terminal Port option defaults.

Two methods can be used to restore access to the ATI. Both methods cause a device reset.

- **Reset Terminal Port** – Allows you to only reset the configuration options related to Terminal port usage. No security-related configuration options are changed.
- **Reload Factory Defaults** – Allows you to reload the Default Factory Configurations, resetting all of the configuration areas and control settings for security reasons. This method is useful when the user's passwords have been forgotten.

Refer to Terminal Port Options, Table A-4. To reset Terminal port settings:

▶ Procedure

1. At the async terminal connected to the Terminal port, verify that the Terminal port options are set to the default settings:
   - — Data Rate(Kbps) to 9.6
   - — Character Length to 8
   - — Stop Bits to 1
   - — Parity to None
2. Power the DSU Off and back On. The DSU performs a power-up routine.
3. Immediately after the OK LED turns on, press the Return key 5 times quickly in succession. The System Paused screen appears.
4. Tab to the desired method, and enter yes (or y) for the selected prompt.

If entering yes to prompt . . .	Then all . . .
Reset Terminal Port Options	Terminal port options are set to their factory default values. Refer to Terminal Port Options, Table A-4.
Reload Factory Defaults	Factory default settings contained in the Default Factory Configuration area are loaded in Current, Customer 1, and Customer 2 configuration areas. Any changes to configuration and control settings will be replaced by the factory defaults.

   If no (or n) is entered, or if no selection is made within 30 seconds, the DSU returns to the condition or operation it was in when the system pause was initiated, with the Terminal port data rate returning to its configured rate.
5. If yes (or y) is entered, the DSU resets itself and initiates a Device Self-Test. Connectivity is restored and the Main Menu screen appears.

Messages and Troubleshooting

8

Messages and Troubleshooting

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

- *Alarm Messages*
  - *ASCII Alarms*
  - *ASCII Alarm Messages*
  - *Configuring SNMP Traps*
  - *Dialing Out SNMP Traps*
- *Device Messages*
- *Troubleshooting*

Alarm Messages

Alarm messages and SNMP traps are unsolicited messages sent out from the DSU automatically when the DSU detects conditions set by the user.

ASCII Alarms

Alarm messages are sent out to an ASCII terminal or printer via the Management port if:

- Port Use is configured for Alarms. Refer to Management Port Options, Table A-5.
- Each ASCII Alarm Message to be generated has been enabled. Refer to Network Interface Options, Table A-2, and System Options, Table A-1.
- ASCII Alarm Messages option is enabled. Refer to Alarms & Traps Options, Table A-8.

When individually enabled, a specific alarm is sent at the start of the corresponding alarm condition. If more than one alarm condition exists, only the highest priority alarm will be sent. Any other alarms are sent out when the higher priority alarm clears. An alarm cleared message is sent when the alarm conditions no longer exist.

The dialing out of ASCII Alarm messages, via an external device (e.g. modem) connected to the Management port, can only occur when, in addition to the above, the:

- External Device Commands is set to AT or Other. Refer to External Device Options, Table A-6.
- Alarm and Trap Dial-Out is enabled. Refer to Alarms & Traps Options, Table A-8.

ASCII Alarm Messages

Refer to the *Entering Device and System Information* section of Chapter 3 for device name information. Each ASCII alarm message is preceded by the device name and a time stamp. The time stamp *(ddd:hh:mm)* represents the cumulative number of days, hours, and minutes since the DSU's last reset. The time resets to zero on power up or reset. An ASCII alarm message displays similar to this example:

NE815378 283:14:57 Crossed Pair condition has been detected on the DDS Network Interface

The following messages can be generated by the DSU and are listed in high to low priority order:

- A Crossed Pair condition has been detected on the DDS Network Interface.
- A No Signal (NS) condition has been detected on the DDS Network Interface.
- An Out of Service (OOS) condition has been detected on the DDS Network Interface.
- An Out of Frame (OOF) condition has been detected on the DDS Network Interface.
- An Excessive Bipolar Violations (BPV) condition has been detected on the DDS Network Interface.
- An In-Band Framing Error condition has been detected on the DDS Network Interface.

Configuring SNMP Traps

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

To configure the DSU 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 DSU.
- Enter an IP address and network destination for each SNMP manager specified.
- Select the type of SNMP traps to be sent from the DSU.

To configure SNMP Traps, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → SNMP & Communication → SNMP Traps

Refer to SNMP Traps Options, Table A-12.

Dialing Out SNMP Traps

Configure the SNMP traps before performing this procedure.

▶ Procedure

1. Configure the phone directories to use when dialing out SNMP traps through the Management port and a connected external device. Refer to the *Call Setup* section in Chapter 3.
2. Use the Alarms & Traps Options to enable the DSU's automatic call initiation to a remote device with Alarm & Trap Dial-Out, Call Retry, and Alternate Dial-Out Directory. Follow this menu selection sequence:

   Main Menu → Configuration → Load Configuration From → Edit → Alarms & Traps

Refer to Alarms & Traps Options, Table A-8.

Device Messages

The Device Messages in Table 8-1, listed in alphabetical order, may appear in the messages area at the bottom of the ATI screens.

Table 8-1. Device Messages (1 of 2)

Device Message	What Message Indicates	What To Do
Blank Entries Removed	New had been selected from the Administer Logins screen, no entry was made, and Save was selected.	■ No action needed. ■ Reenter the Login ID, Password, and Access Level.
Command Complete	Action requested has successfully completed.	No action needed.
Invalid Character (*x*)[1]	A nonprintable ASCII character has been entered.	Reenter information using valid characters.
Invalid – Network Initiated CSU (or DSU) Loopback Active	Network-initiated loopback was in progress when another selection was made.	No action needed.
Invalid Password	Login is required and an incorrect password was entered; access is denied.	■ Try again. ■ Contact your system administrator to verify your password.
Invalid – [Test] Already Active	[Test] can be a CSU, DSU, or DTE Local Loopback, or a Send 511 or Monitor 511. The [test] was already in progress when another selection was made.	■ Allow test to continue. ■ Select another test. ■ Stop the test.
Invalid Test Combination	A loopback or 511 pattern test was in progress when Start was selected to start another test, or was active on the same or another interface when Start was selected.	■ Wait until other test ends and message clears. ■ Abort all tests from the Test menu screen. ■ Stop the test from the same screen the test was started from.
Limit of six Login IDs reached	An attempt to enter a new login ID was made, and the limit of six login/password combinations has been reached.	1. Delete another login/password combination. 2. Reenter the new login ID.
No Security Records to Delete	Delete was selected from the Administer Login screen, and no security records had been defined.	■ No action needed. ■ Enter a security record.

[1] *x* is the character not being accepted.

Table 8-1. Device Messages (2 of 2)

Device Message	What Message Indicates	What To Do
Password Matching Error – Re-enter Password	Password entered in the Re-enter Password field of the Administer Logins screen does not match what was entered in the Password field.	■ Try again. ■ Contact your system administrator to verify your password.
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.	■ Contact service provider if test initiated by the network. ■ Wait until the other test ends and message clears. ■ Cancel all tests from the Test screen. ■ Stop the test from the same screen the test was started from.

Troubleshooting

This DSU is designed to provide you with many years of trouble-free service. If a problem occurs, however, refer to Table 8-2 for possible solutions.

Table 8-2. Troubleshooting (1 of 2)

Symptom	Possible Cause	Solutions
Alarm LED is on.	One of several alarm conditions exists. Health and Status displays the alarm condition.	Refer to Health and Status Messages, Table 6-1, for recommended action.
Cannot access the DSU via the ATI.	Login or password is incorrect, Terminal port is misconfigured, or the DSU otherwise configured so it prevents access.	1. Power the DSU on and off and try again. 2. If problem recurs, try to access the ATI through a Telnet session, if enabled. 3. Do a Device Reset. Refer to the *Device Reset* section of Chapter 7.
Device Fail appears on the System and Test Status screen under Self-Test results.	The DSU detects an internal hardware failure.	■ Power the DSU off and on and try again. ■ Contact your service representative.

Table 8-2. Troubleshooting (2 of 2)

Symptom	Possible Cause	Solutions
An LED is not lit.	LED is burned out.	Run the Lamp test. If the LED in question does not flash with the other LEDs, then contact your service representative.
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.	■ Check the wall receptacle power by plugging in some equipment that is known to be working. ■ Check the circuit breaker. ■ Verify that your site is not on an energy management program.
Not receiving data; DSU is not responding.	■ DDS line rate/speed has changed. ■ Excessive BPVs causing DSU to become stuck in Autobaud mode. ■ Excessive Loop Loss causing DSU to become stuck in Autobaud mode.	1. Verify that your subscriber loop is running at 56 or 64 CC kbps. 2. Verify that the DSU is set to the same rate as your subscriber loop. The DSU's rate is displayed on the Network Interface Status screen. 3. If getting Excessive BPVs, verify that you do not have a bad cable. If the cable is good, contact the network provider. 4. If getting excessive Loop Loss (dB) indications, install a higher quality cable. Refer to Model 7610 DSU LADS Connection Distances, Table 3, in the Start-Up Instructions. 5. If the DDS Line Rate (Kbps) field shows Autobaud, the DSU may be stuck in Autobaud mode. Configure Line Rate (Kbps) for 56 or 64 kbps. 6. Run Loopback tests. Refer to the *Tests Available* section of Chapter 7.
Power-Up Self-Test fails. Only Alarm LED is on after power-up.	The DSU has detected an internal hardware failure.	■ Reset the DSU and try again. ■ Contact your service representative.

Configuration Option Tables

A

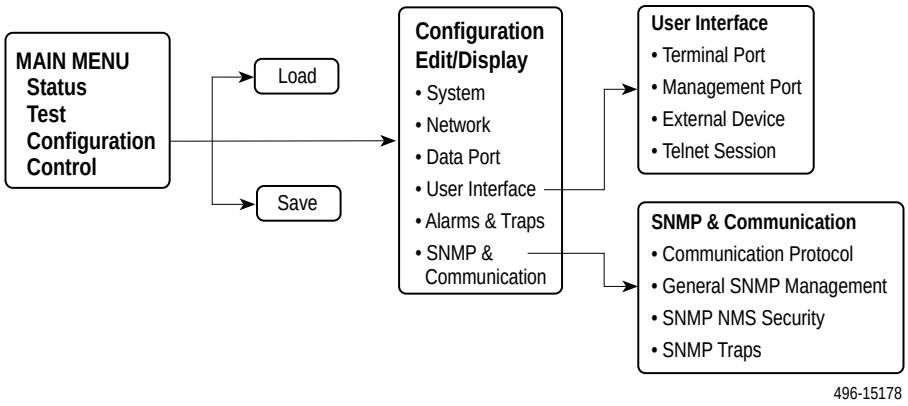
Configuration Option Tables Overview

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 . . .
System	System Options, Table A-1	General system options
Network	Network Interface Options, Table A-2	DDS network interface
Data Port	Data Port Options, Table A-3	User data on DTE port
User Interface	■ Terminal Port Options, Table A-4 ■ Management Port Options, Table A-5 ■ External Device Options, Table A-6 ■ Telnet Sessions Options, Table A-7	Access to the ATI
Alarms & Traps	Alarms & Traps Options, Table A-8	ASCII alarms and SNMP traps initiated by the DSU
SNMP & Communication	■ Communication Protocol Options, Table A-9 ■ General SNMP Management Options, Table A-10 ■ SNMP NMS Security Options, Table A-11 ■ SNMP Traps Options, Table A-12	Management support through SNMP and Telnet session and communication protocols

NOTE:

All changes to configuration options must be saved. Refer to the *Saving Configuration Options* section of Chapter 3.



System Options Menu

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

Main Menu → Configuration → Load Configuration From → Edit → System

Table A-1. System Options (1 of 3)

Operating Mode
Possible Settings: **DDS**, **LADS** Default Setting: **DDS**
The unit's operating mode depends upon the DSU's application. **DDS** – Standard DDS network operation. The operating rate is either 56 kbps or 64 kbps CC. **LADS** – The Local Area Data Set operating mode requires that the local and remote units are connected directly to each other. This is a point-to-point application; also known as LDM.

Table A-1. System Options (2 of 3)

DDS Line Rate (Kbps)
Possible Settings: **56, 64CC**, **Autobaud** Default Setting: **Autobaud**
The unit starts up with Autobaud. When the DDS line rate obtained from the service provider is detected, Autobaud is replaced with the actual rate. ■ DDS Line Rate (Kbps) option appears when Operating Mode is set to DDS. NOTES: – Setting the actual data rate results in minimum power-up time. (If both DSUs use Autobaud, the process can take several minutes.) Configure the actual data rate after initial installation. – The clock rates generated by the DSU at the DTE interface (TXC and RXC) equal the operating rate minus the configured rate of 1600, 4000, or 8000 bps for the IMC, if enabled. Refer to the In-Band Management Channel Rate (bps) option in Table A-2. **56** – 56 kbps line rate. **64CC** – 64 kbps Clear Channel on a 72 kbps circuit. **Autobaud** – This setting is automatically changed to the actual operating line rate of 56 kbps or 64CC as soon as the signal is detected.
LADS Timing
Possible Settings: **Internal, External, Receive** Default Setting: **Internal**
Determines the timing source for the unit. ■ LADS Timing option appears when Operating Mode is set to LADS. **Internal** – Timing derived from the unit's local clock. Use this setting for the LADS primary timing unit that establishes the timing for both point-to-point units. **External** – Timing is derived from the external clock provided by the DTE connected to the V.35 interface on circuit CT113 (pins U, W). NOTE: The valid rate generated by the DTE must be equal to the LADS line rate minus the configured rate of 1600, 4000, or 8000 bps for the IMC, if enabled. Refer to the In-Band Management Channel Rate (bps) option in Table A-2. **Receive** – Timing is derived from the line receive signal unless the unit is running diagnostic tests. During the tests, the timing source is the internal clock. This setting should be used for a LADS secondary timing unit.
LADS Line Rate (Kbps)
Possible Settings: **56, 64** Default Setting: **64**
Line operating rate for LADS operation. ■ LADS Line Rate (Kbps) option appears when Operating Mode is set to LADS. **56** – 56 kbps line rate. Provides increased distance for the LADS applications. **64** – 64 kbps line rate.

Table A-1. System Options (3 of 3)

Test Timeout
Possible Settings: **Enable**, **Disable** Default Setting: **Enable**
Allows user-initiated tests to end automatically. Recommend enabling when the unit is managed remotely through the IMC to avoid the requirement to terminate the test manually. **Enable** – User-initiated loopback and pattern tests end when test duration is reached. **Disable** – Tests can be terminated manually from the Network Tests screen. Refer to the *Network Tests* section of Chapter 7. NOTE: Tests commanded by the DTE or network-initiated tests are not affected by this test timeout.
Test Duration (min)
Possible Settings: **1–120** Default Setting: **10**
Number of minutes for a test to be active before automatically ending. ■ Test Duration (min) option appears when Test Timeout is enabled. **1 to 120** – Amount of time in minutes for a user-initiated test to run before terminating.
Security Violation Alarm
Possible Settings: **Enable**, **Disable** Default Setting: **Enable**
Issues an alarm when access to the unit is attempted and fails. **Enable** – Alarm generated when a security violation is detected. Refer to the *Trap: authentificationFailure* section of Appendix D for possible alarm causes. **Disable** – No alarm generated for a security violation.

Network Interface Options Menu

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

Main Menu → *Configuration* → *Load Configuration From* → *Edit* → *Network*

Table A-2. Network Interface Options (1 of 4)

Network-initiated DSU Loopback (64K CC)
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Indicates whether the access unit responds to a DSU latching loopback sequence sent by the network as specified by TR62310. ▪ Network-initiated DSU Loopback (64K CC) option appears when Operating Mode is set to DDS in Table A-1. **Enable** – Responds to network-initiated commands to start and stop a latching DSU loopback. **Disable** – DSU will not respond to a DSU loopback initiated by the network.
Data Scrambling (64K CC)
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Data scrambling is used to suppress the possible simulation of network-initiated DSU latching loopback commands by application data. ▪ Data Scrambling (64K CC) option appears when Operating Mode is set to DDS in Table A-1. **Enable** – Enables data scrambling. The local and remote units must be set the same. **Disable** – No data scrambling.
V.54 Initiated DSU Loopback
Possible Settings: **Enable, Disable** Default Setting: **Disable**
When enabled, user data is looped back to the network when a V.54 Loop Up sequence is received. The DSU loopback ends when a V.54 Loop Down sequence is detected. **Enable** – DSU loopback can be initiated or terminated by a remote unit sending in-band V.54 Loop 2 Up or Down sequences. **Disable** – V.54 Loop 2 sequences are ignored.
In-Band Management Channel Rate (bps)
Possible Settings: **Disable, 1600, 4000, 8000** Default Setting: **Disable**
The IMC provides a non-disruptive management channel to the remote DSU and uses a portion of the DTE line rate. **Disable** – The IMC is inactive. **1600, 4000, or 8000** – Sets the amount of the line rate in bps to allocate to the IMC. NOTE: The local and remote units must be set the same.

Table A-2. Network Interface Options (2 of 4)

IMC IP Address
Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the Internet Protocol address used to access the unit via the IMC interface. ■ IMC IP Address option does not appear when the In-Band Management Channel Rate (bps) is disabled. **000.000.000.000 – 223.255.255.255** – 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. **Clear** – Clears the IMC IP address and sets to all zeros.
IMC Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the subnet mask used to access the unit via the IMC interface. ■ IMC Subnet Mask option does not appear when the In-Band Management Channel Rate (bps) is disabled. **000.000.000.000 – 255.255.255.255** – Set the IMC interface subnet mask. The range for each byte is 000 to 255. **Clear** – Clears the IMC Subnet Mask and sets to all zeros. When the subnet mask is all zeros, the device creates a default subnet mask based on the class of IP address: – Class A defaults to 255.000.000.000 – Class B defaults to 255.255.000.000 – Class C defaults to 255.255.255.000
IMC Routing Information Protocol
Possible Settings: **None, Proprietary** Default Setting: **Proprietary**
The RIP routes IMC management information between devices. ■ IMC Routing Information Protocol does not appear when the In-Band Management Channel Rate (bps) option is disabled. **None** – No routing protocol. **Proprietary** – Uses proprietary variant of RIP Version 1 to enable the routing of IP traffic between Paradyne devices.
Cross Pair Detection Alarm
Possible Settings: **Enable, Disable** Default Setting: **Enable**
When a crossed pair condition is detected on the network interface, an ASCII alarm is generated. ■ Cross Pair Detection Alarm option appears when the Operating Mode is set to DDS in Table A-1. **Enable** – Generates an ASCII alarm when a crossed pair condition is detected. **Disable** – No ASCII alarm is generated. NOTE: Additional settings are required to send out an ASCII alarm. Refer to the *Alarm Messages* section in Chapter 8.

Table A-2. Network Interface Options (3 of 4)

No Signal Alarm
Possible Settings: **Enable, Disable** Default Setting: **Enable**
When a NS condition is detected on the network interface, an ASCII alarm is generated. **Enable** – Generates an ASCII alarm when a no signal condition is detected. **Disable** – No ASCII alarm is generated. NOTE: Additional settings are required to send out an ASCII alarm. Refer to the *Alarm Messages* section in Chapter 8.
Out of Service Alarm
Possible Settings: **Enable, Disable** Default Setting: **Enable**
When an OOS condition is detected on the network interface, an ASCII alarm is generated. ■ Out of Service Alarm option appears when the Operating Mode is set to DDS in Table A-1. **Enable** – Generates an ASCII alarm when an out of service condition is detected. **Disable** – No ASCII alarm is generated. NOTE: Additional settings are required to send out an ASCII alarm. Refer to the *Alarm Messages* section in Chapter 8.
Out of Frame Alarm
Possible Settings: **Enable**, **Disable** Default Setting: **Enable**
When an OOF condition is detected on the network interface, an ASCII alarm is generated. **Enable** – Generates an ASCII alarm when an out of frame condition is detected on the network interface. **Disable** – No ASCII alarm is generated. NOTE: Additional settings are required to send out an ASCII alarm. Refer to the *Alarm Messages* section in Chapter 8.
Excessive BPV Alarm
Possible Settings: **Enable**, **Disable** Default Setting: **Enable**
When a Bipolar Violation condition is detected on the network interface, an ASCII alarm is generated. **Enable** – Generates an ASCII alarm when an excessive BPV condition is detected. **Disable** – No ASCII alarm is generated. NOTE: Additional settings are required to send out an ASCII alarm. Refer to the *Alarm Messages* section in Chapter 8.

Table A-2. Network Interface Options (4 of 4)

In-Band Framing Alarm
Possible Settings: **Enable**, **Disable** Default Setting: **Enable**
When an in-band framing condition is detected on the network interface, an ASCII alarm is generated. ■ In-Band Framing Alarm option does not appear when the In-Band Management Channel Rate (bps) is disabled. **Enable** – Generates an ASCII alarm when a in-band framing condition is detected. **Disable** – No ASCII alarm is generated. NOTE: Additional settings are required to send out an ASCII alarm. Refer to the *Alarm Messages* section in Chapter 8.

Data Port Options Menu

For Data Port Options, refer to Table A-3. To access the Data Port Options screen, follow this menu selection sequence:

Main Menu → *Configuration* → *Load Configuration From* → *Edit* → *Data Port*

Table A-3. Data Port Options (1 of 3)

Invert Transmit Clock
Possible Settings: **Enable, Disable** Default Setting: **Disable**
The DSU clock provided on Interchange Circuit CT114, Transmit Signal Element Timing DCE source (TXC), is phase inverted with respect to Interchange Circuit CT103, Transmitted Data (TXD). Recommended when data errors are occurring due to long cable lengths. **Enable** – The DSU-supplied clock is phase inverted with respect to the transmitted data TXD. **Disable** – The clock supplied by the DSU on TXC is normal (i.e., not inverted).
Port (DTE) Initiated Loopbacks
Possible Settings: **Disable**, **Local, Remote, Both** Default Setting: **Disable**
Specifies whether the DTE can initiate and terminate local and/or remote loopbacks. The DTE loopback control is done through the Interchange Circuits specified by the V.54 standard. NOTE: Refer to the *Loopbacks* section of Chapter 7. **Disable** – No local or remote loopbacks can be initiated by the DTE. **Local** – A local loopback can be controlled by the DTE, via the Interchange Circuit LL (CT141), as specified by V.54. The DTE port remains in loopback as along as LL remains on. Aborting the loopback from the ATI has no effect. **Remote** – A remote digital loopback can be controlled by the DTE, via Interchange Circuit RL (CT140), as specified by V.54. The remote equipment must be able to detect the in-band V.54 loopback sequence. **Both** – Both the local and remote loopbacks can be controlled by the DTE.
Bilateral Loopback
Possible Settings: **Enable, Disable** Default Setting: **Disable**
When a DSU loopback is initiated, a local DTE loopback is also automatically initiated. A Bilateral Loopback can be started by the ATI/NMS or by detection of a V.54 Loop 2 Up sequence. **Enable** – When Bilateral Loopback is enabled, running a DSU loopback also automatically starts a local loopback. The local loopback ends when the DSU loopback terminates. **Disable** – Running a DSU loopback does not start a local loopback. NOTE: Refer to the *Loopbacks* and the *Network Tests* sections of Chapter 7.

Table A-3. Data Port Options (2 of 3)

Carrier Control by RTS
Possible Settings: **Constant**, **Switched** Default Setting: **Constant**
Simulates Constant or Switched Carrier operation. ■ Carrier Control by RTS option appears when In-Band Management Channel Rate (bps) is disabled in Table A-2. **Constant** – The internal RTS is forced on and the DSU is in a constant Data Mode on the transmit line. The external RTS lead is ignored. The actual signal on the line is either all ones (DMI) or DTE transmitted data. **Switched** – RTS is monitored and CMI codes are transmitted when RTS is off.
CTS Control
Possible Settings: **Standard**, **Follow RTS, Forced On, Circuit Assurance** Default Setting: **Standard**
Specifies the operation of the Interchange Circuit CT106, Clear to Send (CTS), which is an output from the DSU. **Standard** – CTS follows the internal RTS with a fixed delay, except that CTS will be off when a network interface related alarm is detected or a test is active. The active test may be initiated locally, remotely, or by the network. **Follow RTS** – CTS follows the external RTS lead without delay, regardless of alarms and tests. **Forced On** – CTS is always forced on after the unit is powered up with a successful self-test. **Circuit Assurance** – With circuit assurance, CTS operates the same as the Standard option, except that CTS will also be deasserted when CMI codes are being received.
RLSD Control
Possible Settings: **Standard**, **Forced On** Default Setting: **Standard**
Specifies the operation of the Interchange Circuit CT109, Received Line Signal Detector (RLSD or CD), which is an output from the DSU. **Standard** – RLSD is asserted when Data Mode is on the receive line. RLSD deasserts when a DDS facility alarm is detected or the DSU is receiving CMI codes. **Forced On** – RLSD is forced on after the unit is powered up with a successful self-test.
DSR Control
Possible Settings: **Standard**, **Forced On, On During Test** Default Setting: **Standard**
Specifies the operation of the Interchange Circuit CT107, Data Set Ready (DSR), which is an output from the DSU. **Standard** – DSR is always asserted, except when a DDS facility alarm is reported or the DSU is in Test mode. **Forced On** – DSR is forced on after the unit is powered up with a successful self-test. **On During Test** – DSU operates the same as the Standard option, except that DSR remains asserted when the DSU is in Test mode to allow the DTE to send test patterns.

Table A-3. Data Port Options (3 of 3)

Monitor DTR
Possible Settings: **Enable**, **Disable** Default Setting: **Enable**
Indicates to the DSU whether to monitor the Interchange Circuit CT108, Data Terminal Ready (DTR), from the DTE. **Enable** – The DSU monitors the state of DTR on the User Data (DTE) port. Based on the Link Traps option setting in Table A-12, the DSU uses the DTR circuit to trigger a Link Up/Down SNMP trap and a Health and Status message. **Disable** – DTR is not monitored by the DSU. Use when a DTE does not provide the DTR lead at the interface.

User Interface Options Menu

The User Interface Options Menu includes the following:

- Terminal Port Options, Table A-4
- Management Port Options, Table A-5
- External Device Options, Table A-6
- Telnet Session Options, Table A-7

Terminal Port Options

To access the Terminal Port Options screen, follow this menu selection sequence:

Main Menu → *Configuration* → *Load Configuration From* → *Edit* → *User Interface* → *Terminal Port*

Table A-4. Terminal Port Options (1 of 3)

Data Rate (Kbps)
Possible Settings: **2.4, 4.8, 9.6, 14.4, 19.2, 28.8, 38.4** Default Setting: **9.6**
Data rate in kbps on the Terminal port. **2.4 to 38.4** – Selects a Terminal port data rate from 2.4 to 38.4 kbps.
Character Length
Possible Settings: **7, 8** Default Setting: **8**
Specifies the number of bits needed to represent one character, including the parity bit. **7 or 8** – Sets the bits per character.

Table A-4. Terminal Port Options (2 of 3)

Parity
Possible Settings: **None, Even, Odd** Default Setting: **None**
Specifies Parity for the Terminal port. **None** – Provides no parity. **Even** – Parity is even. **Odd** – Parity is odd.
Stop Bits
Possible Settings: **1**, **1.5, 2** Default Setting: **1**
Provides the number of stop bits for the Terminal port. **1, 1.5, or 2** – Selects the number of stop bits.
Monitor DTR
Possible Settings: **Enable**, **Disable** Default Setting: **Enable**
Specifies monitoring of the Data Terminal Ready (DTR) control lead. **Enable** – Standard operation of the DTR control lead. **Disable** – DTR is ignored. Some external device connections may require this setting.
Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Used to secure access to the ATI through the Terminal port. Login IDs are created with a password and access level. **Enable** – Security is enabled. When ATI access is attempted through the Terminal port, a screen appears that requires a Login ID and password. **Disable** – Main menu appears with no Login required. NOTE: Refer to the *Creating a Login* section of Chapter 4.
Port Access Level
Possible Settings: **Level 1**, **Level 2, Level 3** Default Setting: **Level 1**
The Terminal port access level is interrelated with the access level of the Login ID. **Level 1** – This is the highest access level. If Login Required is disabled, the Terminal port access is level 1. If Login Required is enabled, the effective level is the Login ID access level. **Level 2** – This access level overrides a Login ID with an access level 1. If a Login ID has an access level of 3, the effective access level is 3. **Level 3** – This access level becomes the effective access level and overrides a Login ID with an access level of 1 or 2. NOTE: Refer to the *ATI Access* section of Chapter 4 for access level details.

Table A-4. Terminal Port Options (3 of 3)

Inactivity Timeout
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Provides automatic logoff of an ATI session through the Terminal Port. When the session is closed, User Interface Idle appears on the screen and the unit toggles the Terminal port DSR lead. **Enable** – The ATI session terminates automatically after the Disconnect Time set in the next option. When the session was occurring over an external modem connected to the Terminal port, the modem will interpret the DSR toggle as DTR being dropped and disconnect. **Disable** – An ATI session through the Terminal port will remain active indefinitely.
Disconnect Time(minutes)
Possible Settings: **range 1 – 60** Default Setting: **5**
Number of minutes of inactivity before the ATI session terminates automatically. Timeout is based on no keyboard activity. ■ Disconnect Time(minutes) option appears when Inactivity Timeout is enabled. **1 to 60** – The ATI user session is closed after the selected number of minutes.

Management Port Options

To access the Management Port Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → User Interface → Management Port

Table A-5. Management Port Options (1 of 3)

Port Use
Possible Settings: **Net Link**, **Alarms, None** Default Setting: **Net Link**
The Management port provides a choice of functions. **Net Link** – The Management port is the network communication link and provides connectivity to an IP network to support SNMP managers and Telnet sessions. **Alarms** – The Management port is dedicated as an alarm port and sends out ASCII alarm messages. **None** – Disables the Management port. ■ No other fields in this table will appear when set to None.

Table A-5. Management Port Options (2 of 3)

Port Type
Possible Settings: **Asynchronous, Synchronous** Default Setting: **Synchronous**
Establishes asynchronous or synchronous communication for the Management port. ■ Port Type option can be changed only when Port Use is set to Net Link. **Asynchronous** – Port set for asynchronous communication. ■ Asynchronous displays when Port Use is set to Alarms and cannot be changed. **Synchronous** – Port set for synchronous communication.
Clock Source
Possible Settings: **Internal**, **External** Default Setting: **Internal**
Specifies internal or external clocking. ■ Clock Source option appears when Port Type is set to Synchronous. **Internal** – Clocking is provided internally. **External** – Clocking is provided externally. The Management port is always defined as a DCE. This option setting forces the Management port to use external transmit clocking (XTXC or TT) from a connected device (DTE).
Data Rate (Kbps)
Possible Settings: **2.4, 4.8, 9.6**, **14.4, 19.2, 28.8, 38.4** Default Setting: **9.6**
Specifies the Management port data rate in kbps. ■ Data Rate (Kbps) option does not appear when Port Type is set to Synchronous with Clock Source set to External. **2.4 to 38.4** – Selects a Management port data rate from 2.4 to 38.4 kbps. ■ 2.4 kbps and 4.8 kbps only appear when Port Type is set to Asynchronous.
Character Length
Possible Settings: **7, 8** Default Setting: **8**
Specifies the number of bits needed to represent one character. ■ Character Length option appears when Port Type is set to Asynchronous. **7 or 8** – Sets the bits per character.
Parity
Possible Settings: **None, Even, Odd** Default Setting: **None**
Specifies the Parity on the Management port. ■ Parity option appears when Port Type is set to Asynchronous. **None** – Provides no parity. **Even** – Parity is even. **Odd** – Parity is odd.

Table A-5. Management Port Options (3 of 3)

Stop Bits
Possible Settings: **1**, **1.5, 2** Default Setting: **1**
Provides the number of stop bits for the Management port. ■ Stop Bits option appears when Port Type is set to Asynchronous. **1, 1.5, or 2** – Selects the number of stop bits.
Monitor DTR
Possible Settings: **Enable**, **Disable** Default Setting: **Enable**
Specifies monitoring of the Data Terminal Ready (DTR) control lead. ■ Monitor DTR option appears when Port Type is set to Asynchronous. **Enable** – Standard operation of the DTR control lead. **Disable** – DTR is ignored. Some external device connections may require this setting.
Routing Information Protocol
Possible Settings: **None**, **Proprietary** Default Setting: **None**
Specifies the routing protocol between devices through the Management port. ■ Routing Information Protocol appears when Port Use is set for Net Link. **None** – No routing protocol; use None when the device connected to the Management port is not a Model 7610. **Proprietary** – Uses proprietary variant of RIP Version 1 to enable the routing of IP traffic between Paradyne devices.

External Device Options for the Management Port

To access the External Device Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → User Interface → External Device

Table A-6. External Device Options (1 of 3)

External Device Commands
Possible Settings: **Disable, AT, Other** Default Setting: **Disable**
Specifies the type of external device commands to be sent out the Management port. NOTE: The Management port DTR lead is monitored to detect loss of the external device connection. The external device DSR lead must be connected to the Management port's DTR lead, via a standard EIA-232 crossover cable, and the device must be configured to wink DSR on disconnect. **Disable** – No external device commands will be sent out the Management port. ■ No other options in this table will appear. **AT** – Standard AT commands are sent out the Management port to control an external device, such as a modem. When establishing a connection, the AT dial command "ATD" will precede the phone number from the dial directory. ■ The next option, Dial-In Access, is available when External Device Commands is set to AT; no other options in this table will appear. **Other** – Commands configured by the user are sent out the Management port.
Dial-In Access
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Controls external device dial-in access through the Management port. ■ Dial-In Access option appears when External Device Commands is set to AT. **Enable** – Answers incoming calls from an external device and establishes a connection to a remote terminal or IP network. Refer to the Port Use option in Table A-5 for the Management port functions. **Disable** – Incoming calls from an external device are not answered.
Connect Prefix
Possible Settings: **ASCII Text, Clear** Default Setting: [blank]
The connect prefix and directory phone number are used to establish a connection. The connection can be initiated by the user or automatically established for dial out of ASCII alarms or SNMP traps. ■ Connect Prefix option appears when External Device Commands is set to Other. **ASCII Text** – Places a prefix in front of the phone number. Enter a maximum of 20 characters. Refer to the *ASCII Characters* section. **Clear** – Clears the field and sets to none.

Table A-6. External Device Options (2 of 3)

Connect Indication String
Possible Settings: **ASCII Text, Clear** Default Setting: [blank]
Determines if a connection is established. The DSU searches the Management port receive data stream for the connect indication string, and if not received within one minute, the connection times out. The connection can be initiated by the user or automatically established to dial out ASCII alarms or SNMP traps. ■ Connects Indication String option appears when External Device Commands is set to Other. **ASCII Text** – Enter a maximum of 20 characters. Refer to the *ASCII Characters* section for valid ASCII characters and control sequences. **Clear** – Clears the field and sets to no string. The port's RTS lead will be used to determine that a connection has been established.
Escape Sequence
Possible Settings: **ASCII Text, Clear** Default Setting: [blank]
When an external device connection is established, the Escape Sequence can be used to switch an external device to command mode before sending the disconnect command. Refer to Escape Sequence Delay (sec) for delay before and after the Escape Sequence. ■ Escape Sequence option appears when External Device Commands is set to Other. **ASCII Text** – Enter a maximum of 20 characters. Refer to the *ASCII Characters* section for valid ASCII characters and control sequences. **Clear** – Clears the field and sets the escape sequence to none.
Escape Sequence Delay (sec)
Possible Settings: **None**, **0.2, 0.4, 0.6, 0.8, 1.0** Default Setting: **None**
Amount of delay before sending the first character of the escape sequence and after sending the last character. The escape sequence is entered in the previous option. During this delay, no data is sent out the Management port. ■ Escape Sequence Delay (sec) option appears when External Device Commands is set to Other. **None** – No Management port escape sequence delay. **0.2 to 1.0** – Amount of delay in seconds before and after an escape sequence. The delay must be equal to or greater than the escape guard time of the external device.

Table A-6. External Device Options (3 of 3)

Disconnect String
Possible Settings: **ASCII Text, Clear** Default Setting: [blank]
The Disconnect String specifies the command used to disconnect an external device. The external device must be in command mode, so the Escape Sequence is always sent before the Disconnect String. ■ Disconnect String option appears when External Device Commands is set to Other. **ASCII Text** – Enter a maximum of 20 characters. Refer to the *ASCII Characters* section for valid ASCII characters and control sequences. **Clear** – Clears the field and sets to no string. The Management port DSR lead is used to force a disconnect.

Telnet Session Options

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

Main Menu → Configuration → Load Configuration From → Edit → User Interface → Telnet Session

Table A-7. Telnet Session Options (1 of 2)

Telnet Session
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies if the DSU will respond to a Telnet session request from a Telnet client on an interconnected IP network. **Enable** – Allows Telnet sessions between the unit and a Telnet client. **Disable** – No Telnet sessions allowed.
Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Used to secure access to the ATI through a Telnet session. Login IDs are created with a password and access level. Refer to the *Creating a Login* section of Chapter 4. **Enable** – Security is enabled. When access is attempted via Telnet, the user is prompted for a Login ID and password. **Disable** – No Login required for a Telnet session.

Table A-7. Telnet Session Options (2 of 2)

Session Access Level
Possible Settings: **Level 1, Level 2, Level 3** Default Setting: **Level 1**
The Telnet session access level is interrelated with the access level of the Login ID. **Level 1** – This is the highest access level. Access level is determined by the Login ID. If Login Required is disabled, the session access is level 1. **Level 2** – This access level overrides a Login ID with an access level 1. If a Login ID has an access level of 3, the effective access level is 3. **Level 3** – This access level provides the effective access level and overrides the access level of a Login ID. NOTE: Refer to the *ATI Access* section of Chapter 4 for access level details.
Inactivity Timeout
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Provides automatic logoff of a Telnet session. **Enable** – The Telnet session terminates automatically after the Disconnect Time set in the next option. **Disable** – A Telnet session will not be closed due to inactivity.
Disconnect Time (minutes)
Possible Settings: **range 1 – 60** Default Setting: **5**
Number of minutes of inactivity before a Telnet session terminates automatically. Timeout is based on no keyboard activity. ■ Disconnect Time (minutes) option appears when Inactivity Timeout is enabled. **1 to 60** – The Telnet session is closed after the selected number of minutes.

Alarms & Traps Options Menu

For Alarms & Traps Options, refer to Table A-8. To access the Alarms & Traps Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → Alarms & Traps

Table A-8. Alarms & Traps Options (1 of 2)

ASCII Alarm Messages
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Controls the generation and routing of ASCII alarm messages to an ASCII terminal or printer connected to the Management port. Refer to the *Alarm Messages* section of Chapter 8. **Enable** – ASCII alarm messages are generated and sent out when the Management port is configured for Alarms in Management Port Options, Table A-5. ■ The messages are sent out immediately if there is: – No DCE (e.g., modem or PAD) connected to the Management port and External Device Commands option is set to Disable in Table A-6 or – An active connection is already established via an external DCE. ■ If an external device is connected to the Management port with no active connection, the message control is based on the next option, Alarm & Trap Dial-Out. External Device Commands must be configured for AT or Other in External Device Options, Table A-6. **Disable** – ASCII alarm messages are not generated or sent.
Alarm & Trap Dial-Out
Possible Settings: **Enable, Disable** Default Setting: **Disable**
When there is no active connection, this option controls whether generating an ASCII alarm or SNMP trap results in automatic call initiation. **Enable** – Automatically places a call via the external device connected to the Management port. ■ To send out SNMP traps, SNMP Management must be enabled in Table A-10. ■ When Port Use is set to Net Link in Table A-5, up to ten SNMP traps are queued at the interface. ■ The Primary Directory phone number is dialed. Refer to the *Call Setup* section of Chapter 3. ■ Refer to the Call Retry option for handling of incomplete call attempts. **Disable** – Automatic call initiation is disabled and alarm messages are discarded. SNMP traps are retained until a connection is established.

Table A-8. Alarms & Traps Options (2 of 2)

SNMP Trap Disconnect
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines if a Management port external device connection is dropped after sending an SNMP trap. ■ A call established to send out an ASCII alarm always disconnects automatically if the call was initiated automatically. **Enable** – The external device disconnects after sending out an SNMP trap. **Disable** – The external device remains connected and must be disconnected by remote modem or manually. This allows the NMS to poll the DSU after receiving an SNMP trap.
Call Retry
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specify if an unsuccessful call is retried. **Enable** – The call is retried up to five times for each ASCII alarm and each SNMP trap. ■ The following options, Dial-Out Delay Time (min) and Alternate Dial-Out Directory, affect the amount of time before a retry and the number of retries. **Disable** – No retry of an unsuccessful call.
Dial-Out Delay Time (min)
Possible Settings: **1, 2, 3, 4, 5, 6, 7, 8, 9, 10** Default Setting: **5**
This delay applies to both the number of minutes before a new call is initiated for a different alarm and the number of minutes between call retries. Refer to the previous option, Call Retry. **1 to 10** – Number of minutes before a call is initiated or retried.
Alternate Dial-Out Directory
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether an incomplete call initiated for an ASCII alarm or SNMP trap is attempted using the Alternate Directory phone number. ■ Both Alarm & Trap Dial-Out and Call Retry options must be enabled. **Enable** – After attempting to reach the Primary Directory phone number five times, the alternate dial-out directory phone number is dialed five times. NOTE: The Alternate Directory phone number is dialed. Refer to the *Call Setup* section of Chapter 3. **Disable** – No alternate phone number is used.

SNMP & Communication Options Menu

The SNMP & Communications Menu includes the following:

- Communication Protocol Options, Table A-9
- General SNMP Management Options, Table A-10
- SNMP NMS Security Options, Table A-11
- SNMP Traps Options, Table A-12

Communication Protocol Options

To access the Communication Protocol Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → SNMP & Communication → Communication Protocol

Table A-9. Communication Protocol Options (1 of 2)

Management Port IP Address
Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the Internet Protocol address for the Management port. ■ Port Use option must be set to Net Link in Table A-5 for the Management Port IP Address to be effective. **000.000.000.000 – 223.255.255.255** – Sets the Management port IP address. 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. **Clear** – Clears the IP address and sets to all zeros. NOTE: This IP address is also used if the Alternate Directory Phone Number is attempted and the Alternate Mgmt Port IP Address option is all zeros.
Management Port Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the subnet mask needed to access the Management port. **000.000.000.000 – 255.255.255.255** – Set the Management port subnet mask. The range for each byte is 000 to 255. **Clear** – Clears the subnet mask and sets to all zeros. When the subnet mask is all zeros, the device creates a default subnet mask based on the class of IP address: – Class A defaults to 255.000.000.000 – Class B defaults to 255.255.000.000 – Class C defaults to 255.255.255.000

Table A-9. Communication Protocol Options (2 of 2)

Management Port Link Protocol
Possible Settings: **PPP**, **SLIP** Default Setting: **PPP**
Specifies the link layer protocol for the Management port. ■ Port Use option must be set to Net Link in Table A-5 for the Management Port Link Protocol to be effective. **PPP** – Point-to-Point Protocol. **SLIP** – Serial Line Internet Protocol. ■ Port Type option must be set to Asynchronous in Table A-5.
Alternate Mgmt Port IP Address
Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** Default Setting: **000.000.000.000**
IP address to use when a call is initiated using the Alternate Directory Phone Number. If this address is all zeros, the Management Port IP Address is used. **000.000.000.000 – 223.255.255.255** – Sets the alternate Management port IP address. 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. **Clear** – Clears the IP address and sets to all zeros.
Alternate Mgmt Port Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the alternate subnet mask used to access the Management port. Used with the previous option, Alternate Management Port IP Address. **000.000.000.000 – 255.255.255.255** – Sets the management port alternate subnet mask. The range for each byte is 000 to 255. **Clear** – Clears the alternate subnet mask and sets to all zeros. The device creates a default alternate subnet mask based on the class of IP address: – Class A defaults to 255.000.000.000 – Class B defaults to 255.255.000.000 – Class C defaults to 255.255.255.000
Default Network Destination
Possible Settings: **None, Mgmt, IMC** Default Setting: **None**
Specifies where the default network is connected. The routing protocol uses this option to route data with no specific route. **WARNING:** Unroutable data is discarded if the Default Network Destination becomes disabled or the option is set to None. Change the default network destination if the default route is not operational. **None** – No default network destination; unroutable data is discarded. **Mgmt** – The Management port is the default network destination. ■ Port Use option must be set to Net Link in Table A-5. **IMC** – The In-Band Management Channel is the default network destination. ■ In-Band Management Channel Rate(bps) option must be set to 1600, 4000, or 8000 bps in Table A-2.

General SNMP Management Options

To access the General SNMP Management Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → SNMP & Communication → General SNMP Management

Table A-10. General SNMP Management Options (1 of 2)

SNMP Management
Possible Settings: **Enable**, **Disable** Default Setting: **Disable**
Specifies if the DSU can be managed by an SNMP NMS or send out SNMP traps. **Enable** – Enables SNMP management. **Disable** – DSU does not respond to SNMP messages or send out SNMP traps.
Community Name 1
Possible Settings: **ASCII Text, Clear** Default Setting: **Public**
Community Name of external SNMP Managers allowed access to the DSU's MIB. This community name must be supplied by an external SNMP manager attempting to access a MIB object. Level of access is set in the next option, Name 1 Access. **ASCII Text** – Enter a maximum of 255 ASCII printable characters. Refer to the *ASCII Characters* section. **Clear** – Clears the Community Name 1 field.
Name 1 Access
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Set the access level for the Community Name 1 created in the previous option. **Read** – Allows a read-only access (i.e. SNMP Get) to accessible MIB objects. **Read/Write** – Allows both an SNMP Get and Set to MIB objects. Write access allowed to all MIB objects specified as read-write in the MIB RFC.
Community Name 2
Possible Settings: **ASCII Text, Clear** Default Setting: [blank]
Community Name of external SNMP Managers allowed access to the DSU's MIB. This community name must be supplied by an external SNMP manager attempting to access a MIB object. Level of access is set in the next option, Name 2 Access. **ASCII Text** – Enter a maximum of 255 ASCII printable characters. Refer to the *ASCII Characters* section. **Clear** – Clears the Community Name 2 field.

Table A-10. General SNMP Management Options (2 of 2)

Name 2 Access
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Set the access level for the Community Name 2 created in the previous option. **Read** – Allows a read-only access (i.e. SNMP Get) to accessible MIB objects. **Read/Write** – Allows both an SNMP Get and Set to MIB objects. Write access allowed to all MIB objects specified as read-write in the MIB RFC.

SNMP NMS Security Options

To access the SNMP NMS Security Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → SNMP & Communication → SNMP NMS Security

Table A-11. SNMP NMS Security Options (1 of 2)

NMS IP Validation
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines if security checks are performed on the IP address of any SNMP management system that attempts to access the node. **Enable** – Performs security checking. Allows access only if the sending manager's IP address has been entered on the NMS IP address list below. **Disable** – No security checking of incoming SNMP messages.
Number of Managers
Possible Settings: **1, 2, 3, 4, 5, 6, 7, 8, 9, 10** Default Setting: **1**
Set the number of SNMP managers that are authorized to send SNMP messages. The IP address of each SNMP management system must be entered in the next option. **1 to 10** – Specifies the number of SNMP managers allowed to send SNMP messages.

Table A-11. SNMP NMS Security Options (2 of 2)

NMS *n* IP Address
Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** Default Setting: **000.000.000.000**
Enter an IP address for each of the managers set in the previous option. "*n*" is the number of the manager (1 to 10). Use the next option to establish the security level for each SNMP manager. NOTE: When an SNMP message is received from an IP address that does not match the IP address entries in this option, access is denied and an "authenticationFailure" trap is generated. **000.000.000.000 – 223.255.255.255** – Sets the NMS IP address. 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. **Clear** – Clears the IP address and sets to all zeros.
Access Level
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Set the access level for each IP address created in the previous option. **Read** – Allows a read-only access (SNMP Get) to accessible MIB objects. **Read/Write** – Allows both an SNMP Get and Set to MIB objects. Write access allowed to all MIB objects specified as read-write in the MIB RFC. This access level is overriden by the Community Name's access level for the SNMP Manager, if the Community Name access level is Read.

SNMP Traps Options

To access the SNMP Traps Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → SNMP & Communication → SNMP Traps

Table A-12. SNMP Traps Options (1 of 2)

SNMP Traps
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Controls the generation of SNMP trap messages. The options for addresses and types of traps are located in this table. ■ SNMP Management must be enabled in Table A-10. **Enable** – SNMP trap messages are sent out to SNMP managers. ■ If the destination is the Management port and an external device is attached to the Management port, the messages are sent immediately if there is an active connection. Automatic call initiation is based on the Alarm & Trap Dial-Out option in Table A-8. The destination is set with the Trap Manager Destination option. **Disable** – No SNMP trap messages are sent out.
Number of Trap Managers
Possible Settings: **1, 2, 3, 4, 5, 6** Default Setting: **1**
Sets the number of SNMP management systems that will receive SNMP traps. **1 to 6** – Number of trap managers. An NMS IP address is required for each manager.
Trap Manager "*n*" IP Address
Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the Internet Protocol address used to identify each SNMP trap manager. "*n*" represents the number of the manager (from 1 to 6). **000.000.000.000 – 223.255.255.255** – 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. **Clear** – Clears the IP address and sets to all zeros.
Trap Manager "*n*" Destination
Possible Settings: **Default**, **Mgmt, IMC** Default Setting: **Default**
Provides the network destination path of each trap manager. "*n*" is the number of the manager (from 1 to 6). **Default** – Uses the address set in the Default Network Destination in Table A-9. **Mgmt** – The Management port is the network destination. ■ Port Use option must be set to Net Link in Table A-5. **IMC** – The In-Band Management Channel is the default network destination. ■ In-Band Management Channel Rate(bps) option must be set to 1600, 4000, or 8000 bps in Table A-2.

Table A-12. SNMP Traps Options (2 of 2)

General Traps
Possible Settings: **Disable, Warm, AuthFail, Both** Default Setting: **Both**
Determines which SNMP traps are sent to each trap manager. **Disable** – No general trap messages are sent. **Warm** – Sends trap message for "*warmStart*". **AuthFail** – Sends trap message for "*authenticationFailure*". **Both** – Sends both trap messages. NOTE: Refer to *Standards Compliance for SNMP Traps*, Appendix D.
Enterprise Specific Traps
Possible Settings: **Enable, Disable** Default Setting: **Disable**
This option is used to determine if SNMP traps are generated for enterprise-specific events. **Enable** – SNMP traps are generated for enterprise-specific events. NOTE: Refer to the *Traps: Enterprise Specific* section of Appendix D. **Disable** – No enterprise-specific event traps are sent.
Link Traps
Possible Settings: **Disable, Up, Down, Both** Default Setting: **Both**
This option is used to determine if SNMP traps are generated for link up and link down for one of the communication interfaces. **Disable** – No linkUp or linkDown SNMP traps are generated. **Up** – A linkUp trap is generated when the DSU recognizes that one of the communication interfaces is operational. **Down** – A linkDown trap is generated when the DSU recognizes a failure in one of the communication interfaces. **Both** – Sends trap messages for detection of both linkUp and linkDown. NOTE: Refer to the *Traps: linkUp and linkDown* section of Appendix D.
Link Trap Interfaces
Possible Settings: **Network, Port, Both** Default Setting: **Both**
This option determines if the SNMP linkUp, SNMP linkDown, and interface-related enterprise-specific traps are generated for the DDS Network Interface and/or User Data (DTE) port. NOTE: These traps are not supported on the Management port and Terminal port. **Network** – SNMP trap messages are generated for the DDS network interface. **Port** – SNMP trap messages are generated for the User Data (DTE) port. **Both** – SNMP trap messages are generated on both the DDS network interface and the User Date (DTE) port.

ASCII Characters

ASCII characters are divided into ASCII printable characters and ASCII non-printable control sequences.

ASCII printable characters include:

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

ASCII printable characters are valid entries for the following:

- Device Name screen. Refer to the *Entering Device and System Information* section in Chapter 3.
  - — Device Name field
  - — System Name field
  - — System Location field
  - — System Contact field
- Call Directories screen. Refer to the *Call Setup* section in Chapter 3.
  - — Phone Number field
- Administer Logins screen. Refer to the *Creating a Login* section in Chapter 4.
  - — Login ID field
  - — Password field
- External Device Options, Table A-6
  - — Connect Prefix option
  - — Connects Indication String option
  - — Escape Sequence option
  - — Disconnect String option
- General SNMP Management Options, Table A-10
  - — Community Name 1 option
  - — Community Name 2 option

Table A-13 contains non-printable ASCII characters. To form a control sequence, the caret (^) must be followed by one character. In addition to ASCII printable characters, these control sequences are also valid entries in the following:

- Call Directories screen. Refer to the *Call Setup* section in Chapter 3.
  - Phone Number field
- External Device Options, Table A-6
  - Connect Prefix option
  - Connects Indication String option
  - Escape Sequence option
  - Disconnect String option

Table A-13. ASCII Non-Printable Characters

Sequence	ASCII	Hex	Sequence	ASCII	Hex
^A or ^a	SOH	0x01	^Q or ^q	DC1	0x11
^B or ^b	STX	0x02	^ R or ^r	DC2	0x12
^C or ^c	ETX	0x03	^S or ^s	DC3	0x13
^D or ^d	EOT	0x04	^T or ^t	DC4	0x14
^E or ^e	ENQ	0x05	^U or ^u	NAK	0x15
^F or ^f	ACK	0x06	^V or ^v	SYN	0x17
^G or ^g	BEL	0x07	^W or ^w	ETB	0x17
^H or ^h	BS	0x08	^X or ^x	CAN	0x18
^I or ^i	HT	0x09	^Y or ^y	EM	0x19
^J or ^j	LF or NL	0x0A	^Z or ^z	SUB	0x1A
^K or ^k	VT	0x0B	^{ or ^[	ESC	0x1B
^L or ^l	FF or NP	0x0C	^\ or ^|	FS	0x1C
^M or ^m	CR	0x0D	^] or ^}	GS	0x1D
^N or ^n	SO	0x0E	^^ or ^~	RS	0x1E
^O or ^o	SI	0x0F	^-	US	0x1F
^P or ^p	DLE	0x10			

Worksheets

B

Overview

The worksheets in this appendix summarize the configuration options accessed when you select Configuration on the Main Menu. The possible menu selections are displayed with the default settings and the possible settings.

Configuration Worksheets

System	
Configuration Option	**Settings** *Default in [**Bold**]*
Operating Mode	[**DDS**], LADS
DDS Line Rate (Kbps)	56, 64CC, [**Autobaud**]
LADS Timing	[**Internal**], External, Receive
LADS Line Rate (Kbps)	56, [**64**]
Test Timeout	[**Enable**], Disable
Test Duration (min)	1–120, [**10**]
Security Violation Alarm	[**Enable**], Disable

Network Interface	
Configuration Option	**Settings** *Default in [**Bold**]*
Network-initiated DSU Loopback (64K CC)	[**Enable**], Disable
Data Scrambling (64K CC)	Enable, [**Disable**]
V.54 Initiated DSU Loopback	Enable, [**Disable**]
In-Band Management Channel Rate (bps)	[**Disable**], 1600, 4000, 8000
IMC IP Address	[**000.000.000.000**] – 223.255.255.255
IMC Subnet Mask	[**000.000.000.000**] – 255.255.255.255
IMC Routing Information Protocol	None, [**Proprietary**]
Cross Pair Detection Alarm	[**Enable**], Disable
No Signal Alarm	[**Enable**], Disable
Out of Service Alarm	[**Enable**], Disable
Out of Frame Alarm	[**Enable**], Disable
Excessive BPV Alarm	[**Enable**], Disable
In-Band Framing Alarm	[**Enable**], Disable

Data Port	
Configuration Option	**Settings** *Default in [**Bold**]*
Invert Transmit Clock	Enable, [**Disable**]
Port (DTE) Initiated Loopbacks	[**Disable**], Local, Remote, Both
Bilateral Loopback	Enable, [**Disable**]
Carrier Control by RTS	[**Constant**], Switched
CTS Control	[**Standard**], Follow RTS, Forced On, Circuit Assurance
RLSD Control	[**Standard**], Forced On
DSR Control	[**Standard**], Forced On, On During Test
Monitor DTR	[**Enable**], Disable

User Interface	
Configuration Option	**Settings** *Default in [**Bold**]*
Terminal Port	
Data Rate (Kbps)	2.4, 4.8, [**9.6**], 14.4, 19.2, 28.8, 38.4
Character Length	7, [**8**]
Parity	[**None**], Even, Odd
Stop Bits	**[1]**, 1.5, 2
Monitor DTR	[**Enable**], Disable
Login Required	Enable, [**Disable**]
Port Access Level	[**Level 1**], Level 2, Level 3
Inactivity Timeout	Enable, [**Disable**]
Disconnect Time(minutes)	range 1 – 60 [**5**]
Management Port	
Port Use	[**Net Link**], Alarms, None
Port Type	Asynchronous, [**Synchronous**]
Clock Source	[**Internal**], External
Data Rate (Kbps)	2.4, 4.8, [**9.6**], 14.4, 19.2, 28.8, 38.4
Character Length	7, [**8**]
Parity	[**None**], Even, Odd
Stop Bits	[**1**], 1.5, 2
Monitor DTR	[**Enable**], Disable
Routing Management Protocol	[**None**], Proprietary
External Device	
External Device Commands	[**Disable**], AT, Other
Dial-In Access	Enable, [**Disable**]
Connect Prefix	ASCII Text
Connects Indication String	ASCII Text
Escape Sequence	ASCII Text
Escape Sequence Delay (sec)	[**None**], 0.2, 0.4, 0.6, 0.8, 1.0
Disconnect String	ASCII Text
Telnet Session	
Telnet Session	Enable, [**Disable**]
Login Required	Enable, [**Disable**]
Session Access Level	[**Level 1**], Level 2, Level 3
Inactivity Timeout	Enable, [**Disable**]
Disconnect Time (minutes)	range 1 – 60 [**5**]

Alarms & Traps	
Configuration Option	**Settings** *Default in [**Bold**]*
ASCII Alarm Messages	Enable, [**Disable**]
Alarm & Trap Dial-Out	Enable, [**Disable**]
SNMP Trap Disconnect	[**Enable**], Disable
Call Retry	Enable, **[Disable]**
Dial-Out Delay Time (min)	1, 2, 3, 4, **[5]**, 6, 7, 8, 9, 10
Alternate Dial-Out Directory	Enable, [**Disable**]

Management	
Configuration Option	**Settings** *Default in [**Bold**]*
Communication Protocol	
Management Port IP Address	[**000.000.000.000**] – 223.255.255.255
Management Port Subnet Mask	**[000.000.000.000**] – 255.255.255.255
Management Port Link Protocol	**[PPP**], SLIP
Alternate Mgmt Port IP Address	[**000.000.000.000]** – 223.255.255.255
Alternate Mgmt Port Subnet Mask	[**000.000.000.000**] – 255.255.255.255
Default Network Destination	[**None**], Mgmt, IMC
General SNMP Management	
SNMP Management	[**Disable**], Enable
Community Name 1	ASCII Text, **[Public**]
Name 1 Access	[**Read**], Read/Write
Community Name 2	ASCII Text
Name 2 Access	[**Read**], Read/Write
SNMP NMS Security	
NMS IP Validation	Enable, [**Disable**]
Number of Managers	[**1**], 2, 3, 4, 5, 6, 7, 8, 9, 10
NMS “n” IP Address	[**000.000.000.000**] – 223.255.255.255
Access Level	[**Read**], Read/Write
SNMP Traps	
SNMP Traps	Enable, [**Disable**]
Number of Trap Managers	[**1**], 2, 3, 4, 5, 6
Trap Manager “*n*” IP Address	[**000.000.000.000**] – 223.255.255.255
Trap Manager “*n*” Destination	[**Default**], Mgmt, IMC
General Traps	Disable, Warm, AuthFail, [**Both**]
Enterprise Specific Traps	Enable, [**Disable**]
Link Traps	Disable, Up, Down, [**Both**]
Link Trap Interfaces	Network, Port, [**Both**]

MIB Descriptions

C

MIB Description Overview

The following sections show generally how the SNMP DSU supports MIB objects relative to their RFC description. MIBs are available on the World Wide Web site listed on Page A (the reverse side of the title page of this document).

MIB II – RFC 1213 and RFC 1573

The unit supports the following MIB II object groups as defined in RFC 1213 and RFC 1573:

- System Group Objects
- Interfaces Group Objects – Supported for the DDS network interface, User Data (DTE) port, Terminal port, Management port, and the IMC as defined in RFC 1573, the Evolution of the Interfaces Group.
  - Interfaces Group Objects
  - Extension to Interface Table (ifXTable)
  - Interface Stack Group Objects
  - Interface Test Group Objects
- IP Group Objects
- ICMP (Internet Control Management Protocol) Group
- TCP (Transmission Control Protocol) Group
- UDP (User Datagram Protocol) Group
- Transmission Group Objects. Supported on the DDS network interface using the DDS Enterprise MIB. Supported on the User Data (DTE) port, Terminal port, and Management port using the RS-232-like MIB.
- SNMP Group

The following MIB II groups are not supported:

- Address Translation Group
- Exterior Gateway Protocol (EGP) Group

RS-232-Like MIB – RFC 1659

The unit supports RS-232-Like MIB, RFC 1659:

- Number of RS-232-Like Ports Object.
- General Port Table Objects
- Asynchronous Port Table Objects. Not supported for the User Data port.
- Synchronous Port Table Objects. Not supported for the Terminal port.
- Input Signal Table Objects. Not supported for the Management port or Terminal port.
- Output Signal Table Objects. Not supported for the Management port or Terminal port.

Enterprise MIB Objects

The following Paradyne Enterprise MIB Objects are supported by the unit:

- Device Configuration Variable
- Port Usage Table, attp-devPortUsage (attp-interfaces 3)
- DDS Interface Specific Definitions, attp-dds (attp-interfaces 2)
- Device Security, attp-security (att-common 8)
- Device Traps, attp-traps (att-common 9)
- Device Control, attp-control (attp-common 10)

System Group

System Group objects are fully supported by the unit.

Table C-1. System Group Objects

Object	Description	Setting/Contents
sysDescr *(system 1)*	Provides a full name and version identification for the system's hardware and software.	PARADYNE DDS Leased Line DSU*;* Model: 7610-A1-201; S/W Release: *yy.yy.yy;* H/W Revision: *zzzz-zzz;* Serial Number: *sssssss*
sysObjectID *(system 2)*	Identifies the network management subsystem.	1.3.6.1.4.1.1795.1.14.2.5.1.1
sysContact *(system 4)*	Provides the textual identification of the contact person for this managed unit.[1]	ASCII character string, as set by the user.
sysName *(system 5)*	Provides an administratively-assigned name for this managed unit.[1]	ASCII character string, as set by the user.
sysLocation *(system 6)*	Provides the physical location for this managed unit.[1]	ASCII character string, as set by the user.
sysServices *(system 7)*	Functionality supported: ■ **physical (1)** – Layer 1 functionality for all interfaces. ■ **datalink/subnetwork (2)** – Layer 2 functionality (SLIP/PPP) for all management links. ■ **internet (4)** – Layer 3 functionality (IP) for all management links. ■ **end-to-end (8)** – Layer 4 functionality (TCP/UDP) for all management links.	Object is set to 1+2+4+8 (**15**).

[1] The unit supports a 127-character string for this object. An error message is sent to the NMS if an attempt is made to write (set) more than 127 characters.

Interfaces Group

The Interfaces Group as defined in RFC 1573 consists of an object indicating the number of interfaces supported by the unit and an interface table containing an entry for each interface. Since RFC 1573 is an SNMPv2 MIB, it is converted to SNMPv1 for support by the unit. The following table provides clarification for objects contained in the Interfaces group when it is not clear how the object definition in RFC 1573 is supported by the unit.

Table C-2. Interfaces Group Objects (1 of 4)

Object	Description	Setting/Contents
ifNumber *(interfaces 1)*	Specifies the number of interfaces for this unit in the ifTable.	**5**
ifIndex *(ifEntry 1)*	Provides the index to the interface table (ifTable) and to other tables as well. When an unsupported index is entered (e.g., 3 and 5), noSuchName is returned.	Indexes and values: **1** – Management port **2** – Terminal port **4** – DDS network interface **6** – User Data (DTE) port **7** – In-band Management Channel
ifDescr *(ifEntry 2)*	Supplies text for each Interface:	Text Strings for each interface:
	■ Management	■ "Management Port; PARADYNE DDS Leased Line DSU; Hardware Version [*Hardware Revision*]"; Software Version: [*Software Revision*].
	■ Terminal	■ "Terminal Port; PARADYNE DDS Leased Line DSU; Hardware Version [*Hardware Revision*]"; Software Version: [*Software Revision*].
	■ DDS Network	■ "DDS Network; PARADYNE DDS Leased Line DSU; Hardware Version [*Hardware Revision*]"; Software Version: [*Software Revision*].
	■ User Data Port	■ "User Data Port; PARADYNE DDS Leased Line DSU; Hardware Version [*Hardware Revision*]"; Software Version: [*Software Revision*].
	■ In-band Management Channel	■ "In-band Management Channel; PARADYNE DDS Leased Line DSU; Hardware Version [*Hardware Revision*]"; Software Version: [*Software Revision*].

Table C-2. Interfaces Group Objects (2 of 4)

Object	Description	Setting/Contents
ifType *(ifEntry 3)*	Identifies the interface type based on the physical/link protocol(s), right below the network layer.	Supported values: ■ **other(1)** – Used for the DDS network. ■ **ppp(23)** – Used for the In-band Management Channel and for the Management port, when configured for PPP. ■ **slip(28)** – Used for Management port, when configured for SLIP. ■ **rs232(33)** – Used for the Terminal port and the Management port, when not configured as Net Link. ■ **v35(45)** – Used for the User Data port.
ifMtu *(ifEntry 4)*	Identifies the largest datagram that can be sent or received on an interface (Management port or IMC).	Number of octets.
ifSpeed *(ifEntry 5)*	Provides the current bandwidth for the interface in bits per second.	■ Management port – Configured data rate for the port. ■ Terminal port – Configured data rate for the port. ■ DDS – Line rate of 56,000 or 64,000 bps, reflecting the line rate detected by the unit. ■ User data (DTE) port – Current data rate of the port (DDS operating rate minus IMC rate). ■ In-band Management Channel – Configured data rate for the In-band Management Channel.
ifAdminStatus *(ifEntry 7)*	Provides interface status. Supported as read-only.	■ **up(1)** – The interface is enabled. ■ **down(2)** – The interface is disabled.

Table C-2. Interfaces Group Objects (3 of 4)

Object	Description	Setting/Contents
ifOperStatus *(ifEntry 8)*	Specifies the current operational state of the interface.	■ Management port. When configured as Net Link, **up(1)** and **down(2)** are based on the current state of the link-layer protocol. When configured for Alarms, the interface is always **up(1)**. Never in **testing(3)** state. ■ Terminal port. Always **up(1)**; never in **testing(3)** state. ■ User Data Port – **up(1)** – No alarms – **down(2)** – Alarms – **testing(3)** – Test active ■ DDS Network Interface – **up(1)** – DTR on, if supported by the DTE – **down(2)** – DTR off, if supported by the DTE – **testing(3)** – Test active ■ In-band Management Channel. When enabled, up and down are based on the current state of the physical and link layer protocols. – **up(1)** – Operational and no active test on the DDS network interface – **down(2)** – Not operational or disabled – **testing(3)** – Test active on DDS network interface
ifLastChange *(ifEntry 9)*	Indicates the amount of time the interface has been up and running.	Contains the value of sysUpTime object at the time the interface entered its current operational state.
ifInOctets *(ifEntry 10)*	Collects input statistics on data received by the interface. Applies to the IMC and the Management port, if configured for Net Link. When the Management port is not configured as a Net Link, these statistics will not be collected, and an error status will be sent if access is attempted.	An integer number.
ifInUcastPkts *(ifEntry 11)*		
ifInDiscards *(ifEntry 13)*		
ifInErrors *(ifEntry 14)*		
ifInUnknown Protos *(ifEntry 15)*		

Table C-2. Interfaces Group Objects (4 of 4)

Object	Description	Setting/Contents
ifOutOctets *(ifEntry 16)*	Collects output statistics on data received by the interface. Applies to the IMC and the Management port, if configured for Net Link. When the Management port is not configured as a Net Link, these statistics will not be collected, and an error status will be sent if access is attempted.	An integer number.
ifOutUcastPkts *(ifEntry 17)*		
ifOutDiscards *(ifEntry 19)*		
ifOutErrors *(ifEntry 20)*		

Extension to Interface Table (ifXTable)

This extension contains additional objects for the interface table. Supports only the following objects.

Table C-3. Extension to Interface Table (ifXTable)

Object	Description	Setting/Contents
ifName *(ifXEntry 1)*	Provides name of the interface.	Interface text strings: ■ Management Port ■ Terminal Port ■ DDS Network ■ User Data Port ■ In-band Management Channel
ifLinkUpDown-TrapEnable *(ifXEntry 14)*	Indicates whether the link is up or down, or enterprise-specific traps should be generated.	Only supports DDS network and User data port. SNMP Traps must be enabled for the unit. See SNMP Traps Option, Table A-12.
ifHighSpeed *(ifXEntry 15)*	Reflects the ifSpeed setting for the interface.	This object is supported as read-only.
ifConnector-Present *(ifXEntry 17)*	Indicates whether there is a physical connector for the interface.	**true(1)** – Will always have this value for the DDS network, Management port, Terminal port, and User Data port. **false(2)** –Will always have this value for the In-band Management Channel.

Interface Stack Group

The Interface Stack Group is used by the unit to show the relationship between a logical interface and a physical interface. The following table provides clarification for objects contained in the Interface Stack group when it is not clear how the object definition in RFC 1573 is supported by the unit.

Table C-4. Interface Stack Group Objects

Object	Description	Setting/Contents
ifStackHigher-Layer *(ifStackEntry1)*	Provides the index that corresponds to the higher sublevel specified by ifStackLowerLayer.	When the In-band Management Channel is enabled, this object for the DDS network interface is set to the ifIndex of the In-band Management Channel. All other ifStackHigherLayer objects will have a value of zero.
ifStackLower-Layer *(ifStackEntry2)*	Provides the index that corresponds to the lower sublevel specified by ifStackHigherLayer.	When the In-band Management Channel is enabled, this object for the In-band Management Channel is set to the ifIndex of the DDS network interface. All other ifStackLowerLayer objects will have a value of zero.
ifStackStatus *(ifStackEntry3)*	Specifies the stack group's status compared to the interface's ifOperStatus. Supported as a read-only variable.	■ When ifStackStatus set to **active** – maps to ifOperStatus set to **up(1)** or **testing(3)**. ■ When ifStackStatus set to **not in service** – maps to ifOperStatus set to **down(2)**.

Interface Test Table

The unit uses the Interface Test table to provide access to additional tests such as loopbacks and pattern tests, which are not included in the Interfaces Group of MIB II.

Table C-5. Interface Test Group Objects (1 of 2)

Object	Description	Setting/Contents
ifTestID *(ifTestEntry 1)*	Provides a unique identifier for the current request of the interface's test. Ensures that the results of the test are for that request. This handles the rare condition where another SNMP Manager starts a test immediately after completion of a previous test, but before the previous test results are received by the first SNMP manager.	Set by an SNMP Manager before the test is started. The unit then increments the previous value. The value is then checked after the test has completed.

Table C-5. Interface Test Group Objects (2 of 2)

Object	Description	Setting/Contents
ifTestStatus *(ifTestEntry2)*	Indicates the test status of the interface.	■ Set to **inUse(2)** by an SNMP Manager before a test is started. ■ Set to **notInUse(1)** by the unit when the test has completed. Also set to **notInUse(1)** by the unit if the SNMP Manager fails to set an ifTestType within 5 minutes.
ifTestType *(ifTestEntry 3)*	A control variable used to start/stop user-initiated tests on the interface. Provides the following capabilities: ■ Start/stop user data port loopback ■ Start/stop send pattern on the user data port ■ Start/stop the monitor test pattern on the user data port	The following objects use identifiers to control tests on the User Data port interface: ■ **noTest** (0 0) – Stops the test in progress on the interface. ■ **testLoopDTE** (ifTestType 2) – Starts a Local Loopback (DTE) on the interface. ■ **testMon511** (ifTestType4) – Starts a Monitor 511 test on the interface. ■ **testSend511** (ifTestType6) – Starts a Send 511 test on the interface.
ifTestCode *(ifTestEntry 5)*	Contains a code which is more specific about the test results.	Supports the following values: ■ **none** (ifTestCode 1) – No further information is available. Used for send pattern/code and loopback tests. ■ **inSyncNoBitErrors** (ifTestCode 2) – A 511 monitor pattern test has synchronized on the pattern and has not detected any bit errors. ■ **inSyncWithBitErrors** (ifTestCode 3) – A 511 monitor pattern test has synchronized on the pattern and has detected bit errors. ■ **notInSync** (ifTestCode 4) – A 511 monitor test pattern has not synchronized on the requested pattern.
ifTestOwner *(ifTestEntry 6)*	Used by an SNMP Manager to identify the current owner of the test for the interface.	The SNMP Manager sets the object to its IP address when setting ifTestID and ifTestStatus.

Generic Receive Address Table

Not supported by the unit.

IP Group

The Internet Protocol Group objects are supported by the unit for all data paths that are currently configured to carry IP data to/from the unit. All of the objects in the IP Group, except for the IP Address Translation table, are fully supported. The following table provides clarification for objects contained in the IP group when it is not clear how the object definition in MIB II is supported by the unit.

Table C-6. IP Group Objects (1 of 2)

Object	Description	Setting/Contents
ipForwarding *(ip1)*	Specifies whether the unit is acting as an IP gateway for forwarding of datagram received by, but not addressed to, the unit.	Supports only the following value: ■ **forwarding(1)** – The unit is acting as a gateway.
ipAddrTable *(ip20)*	The address table.	Supported.
ipAdEntAddr *(ipAddrEntry 1)*	An IP address supported by the unit which serves as an index to the address table.	Indexes for tables must be unique. Therefore, only one ifIndex can be displayed for each IP address supported by the device. If the same IP address is configured for multiple interfaces, or for default IP addresses, the ipAddrTable will not display all of the interfaces that support a particular IP address.
ipAdEntIfIndex *(ipAddrEntry 2)*	If this object has a greater value than the ifNumber, then it refers to a proprietary interface not currently implemented by the MIB II Interface Group.	None
ipRouteTable *(ip21)*	Supported as read/write. However, use caution when adding or modifying routes. If it is absolutely necessary to add a route, the route should only be added to the connected device (device closest to the destination). Internal routing will continue the route to the other devices.	To delete a route, set object to **invalid**. To modify a route, change fields in the desired entry of the routing table (indexed by ipRouteDest). To add a route, specify values for a table entry for which the index (ipRouteDest) does not already exist. The following objects *must* be specified: ■ ipRouteDest – Serves as an index to the routing table. Only one route per destination can appear in the table. To ensure that no duplicate destinations appear in the routing table, the ipRouteDest object will be treated as described in the IP Forwarding Table MIB (RFC 1354).

Table C-6. IP Group Objects (2 of 2)

Object	Description	Setting/Contents
ipRouteTable *(ip21)* (Continued)		■ ipRouteIfIndex – If this object has a greater value than the ifNumber, then it refers to a proprietary interface not currently implemented by the MIB II Interface Group. Do not delete route entries with an unrecognized ipRouteIfIndex. When setting this object via SNMP, the ipRouteIfIndex value can only assume an appropriate value of IfIndex defined for a particular device type. Objects that will be set to the default value if not specified in the Set PDU used to add a route: ■ ipRouteMetric1 – Defaults to 1 hop. ■ ipRouteType – Defaults to indirect. ■ ipRouteMask – Defaults to what is specified in the MIB description. Objects that are not used by this unit: ■ ipRouteMetric2, ipRouteMetric3, ipRoutemetric4, ipRoutemetric5 – Default to **–1**. ■ ipRouteNextHop – Defaults to **0.0.0.0**. Do not specify the following read-only objects in the Set PDU used to add a route: ■ ipRouteProto – Set to **netmgmt(3**) by the software. May have the following values: – **other(1)** – Temporary route added by IP. – **local(2)** – Route added or changed due to User configuration. – **netmgmt(3)** – Route added or changed by SNMP set. – **icmp(4)** – Route added or changed by ICMP. – **rip(8)** – Route added or changed by RIP (or similar proprietary protocol). ■ ipRouteAge – Reflects the value of the time-to-live for the route (in seconds). Defaults to **999** (permanent route). ■ ipRouteInfo – Unused; set to {0, 0}.

ICMP Group

The ICMP (Internet Control Management Protocol) Group objects are fully supported.

TCP Group

The TCP Group objects are fully supported, with the exception of tcpConnState object, which will be read-only, since deleteTCB (12) is not supported and is the only value which can be set.

UDP Group

The UDP Group objects are fully supported.

Transmission Group

Objects in the Transmission Group are supported on the DDS network interface, User Data port, Management port, and Terminal port. These objects are defined through other Internet-standard MIB definitions rather than within MIB II.

Table C-7. Transmission Group Objects

Object	Description
rs232 *(transmission 33)*	Supported on the User Data port, Management port, and Terminal port. Defined by the RS-232-like MIB (RFC 1659).
enterprise *(transmission 22)*	Supported on the DDS network interface by Paradyne Enterprise MIB.

SNMP Group

The SNMP Group objects that apply to a management agent are fully supported. The following objects apply only to an NMS and return a zero value if accessed.

- snmpInTooBig (snmp 8)
- snmpInNoSuchNames (snmp 9)
- snmpInBadValues (snmp 10)
- snmpInReadOnlys (snmp 11)
- snmpInGenErrs (snmp 12)
- snmpInGetResponses (snmp 18)
- snmpInTraps (snmp 19)
- snmpOutGetRequests (snmp 25)
- snmpOutGetNexts (snmp 26)
- snmpOutSetRequests (snmp 27)

RS-232-Like MIB, RFC 1659

Supported for the User Data port, the Management port, and the Terminal port. RFC 1659 is an SNMPv2 MIB, but is converted to an SNMPv1 MIB to support this unit. This MIB consists of one object and five tables.

Number of RS-232-Like Ports Object

Supported as documented in the RFC.

General Port Table Objects

The General Port Table Objects contains configuration options for the RS-232-Like interfaces. Clarification for objects contained in this table as it applies to the unit is provided below.

Table C-8. General Port Table Objects (1 of 2)

Object	Description	Setting/Contents
rs232PortType *(rs232PortEntry 2)*	Identifies the port hardware type.	Supports only the following values: **rs232(2)** – Identifies the Management port and Terminal port. **v35(5)** – Identifies the synchronous User Data port which is compatible with the V.35 standard.
rs232PortInSig Number *(rs232PortEntry 3)*	Contains the number of input signals (in the input signal table) that can be detected.	The value is **2** for synchronous user data port and **0** for both the Management port and Terminal port.
rs232PortOutSig Number *(rs232PortEntry 4)*	Contains the number of output signals (in the output signal table) that can be asserted.	The value is **3** for synchronous User Data port and **0** for both the Management port and Terminal port.
rs232PortInSpeed *(rs232PortEntry 5)*	Contains the port's input speed in bits per second.	Supports the following speeds for the: ■ User data port: 64,000, 62,400, 60,000, 56,000, 54,400, 52,000, 48,000.[1] ■ Management port: 2400[2], 4800[2], 9600, 14,400, 19,200, 28,800, 38,400. ■ Terminal port: 2400, 4800, 9600,14,400, 19,200, 28,800, 38,400.
[1] The User Data port speed is a read-only value that can only differ from the DDS network speed if the In-band Management Channel is enabled. [2] This speed is only valid when the port is configured for asynchronous operation.		

Table C-8. General Port Table Objects (2 of 2)

Object	Description	Setting/Contents
rs232PortOut Speed *(rs232PortEntry 6)*	Contains the port's output speed in bits per second. The rs232PortOutSpeed object has the same values as the rs232PortInSpeed object.	Supports the following speeds for the: ■ User data port: 64,000, 62,400, 60,000, 56,000, 54,400, 52,000, 48,000.[1] ■ Management port: 2400[2], 4800,[2] 9600, 14,400, 19,200, 28,800, 38,400. ■ Terminal port: 2400, 4800, 9600,14,400, 19,200, 28,800, 38,400.
[1] The User Data port speed is a read-only value that can only differ from the DDS network speed if the In-band Management Channel is enabled. [2] This speed is only valid when the port is configured for asynchronous operation.		

The following are not supported:

- rs232PortInFlowType *(rs232PortEntry 7)*
- rs232PortOutFlowType *(rs232PortEntry 8)*

Asynchronous Port Table Objects

The Asynchronous Port Table Objects contains an entry for the Management port when the port is configured for asynchronous operation and for the Terminal port. For this unit, entries in the table that are counters (rs232AsyncPortEntry 6–8) are used to collect statistics only and are not supported.

Table C-9. Asynchronous Port Table Objects (1 of 2)

Object	Description	Setting/Contents
rs232AsyncPort Bits *(rs232Async PortEntry 2)*	Specifies the number of bits in a character.	Supports only the following values: **7** – 7-bit characters **8** – 8-bit characters
rs232AsyncPort StopBits *(rs232Async PortEntry 3)*	Specifies the number of stop bits supported.	Supports only the following values: **one(1)** – One stop bit **two(2)** – Two stop bits **one-and-half(3)** – One and a half stop bits

Table C-9. Asynchronous Port Table Objects (2 of 2)

Object	Description	Setting/Contents
rs232AsyncPort Parity *(rs232Async PortEntry 4)*	Specifies the type of parity used by the port.	Supports only the following values: **none(1)** – No parity bit **odd(2)** – Odd parity **even(3)** – Even parity
rs232AsyncPort AutoBaud *(rs232Async PortEntry 5)*	Specifies the ability to automatically sense the input speed of the port.	Supports only the following values: **disabled(2)** – Does not support Autobaud.

Synchronous Port Table Objects

The Synchronous Port Table Objects contains an entry for the synchronous user data port and the Management port when this port is configured for synchronous operation. For this unit, entries in the table that are counters (rs232SyncPortEntry 3–7) are used to collect statistics only and are not supported. Clarification for objects contained in this table as it applies to the unit is provided below.

Table C-10. Synchronous Port Table Objects (1 of 2)

Object	Description	Setting/Contents
rs232SyncPort ClockSource *(rs232Sync PortEntry 2)*	Specifies the clock source for the port.	Supports only the following values: **internal(1)** – The port uses an internal clock. **split(3)** – The port uses an external transmit clock and internal receive clock.
rs232SyncPort Role *(rs232Sync PortEntry 8)*	Specifies whether this device interface is a DTE or DCE.	Supports only the following value: **dce(2)** – The port acts as a DCE.
rs232SyncPort Encoding *(rs232Sync PortEntry 9)*	Specifies the bit encoding technique that this port uses.	Supports only the following value: **nrz(1)** – The port uses non-return to zero encoding.
rs232SyncPort RTSControl *(rs232Sync PortEntry 10)*	Specifies the method used to control the RTS signal. Refer to Data Port Options, Table A-3.	Supports only the following values: **controlled(1)** – For User Data port, this value is used when the Data Port option Carrier Control by RTS is set to Switched. **constant(2)** – For User Data port, this value is used when the Data Port option Carrier Control by RTS is set to Constant. This is the only valid value for the Management port.

Table C-10. Synchronous Port Table Objects (2 of 2)

Object	Description	Setting/Contents
rs232SyncPort RTSCTSDelay *(rs232Sync PortEntry 11)*	Reports the interval (in milliseconds) that the port waits after RTS is asserted before asserting CTS.	Supports only the following read-only values: **0** – The port does not have to wait. Only valid for Management port. **integer number** – represents milliseconds. It is only valid for the user data port, when Carrier Control by RTS is set to Switched and corresponds to approximately 21 bit time intervals at the operating DDS rate.
rs232SyncPort Mode *(rs232Sync PortEntry 12)*	Specifies the port's mode of data transfer.	Supports only the following value: **fdx(1)** – Full-duplex

The following are not supported:

- rs232SyncPortIdle Pattern *(rs232SyncPortEntry 13)*
- rs232SyncPortMinFlags *(rs232SyncPortEntry 14)*

Input Signal Table Objects

The Input Signal Table Objects contains entries for the input signals that can be detected by the unit for the synchronous user data port. Clarification for objects contained in this table as it applies to the unit is provided below.

Table C-11. Input Signal Table Objects

Object	Description	Setting/Contents
rs232InSigName *(rs232InSigEntry 2)*	Contains the identification of a hardware input signal.	Supports only the following values: **rts(1)** – Request To Send **dtr(4)** – Data Terminal Ready
rs232InSigState *(rs232InSigEntry 3)*	Contains the current signal state.	Supports only the following values: **on(2)** – The signal is asserted **off(3)** – The signal is deasserted
rs232InSigChanges *(rs232InSigEntry 4)*	Indicates the number of times that a signal has changed from on to off, or off to on.	The object is incremented each time that the signal is sampled (every 100 ms) and the signal state is different from the previous state.

Output Signal Table Objects

The Output Signal Table Objects contains entries for the output signals that can be asserted by the unit, for the synchronous User Data port. Clarification for objects contained in this table as it applies to the unit is provided below.

Table C-12. Output Signal Table Objects

Object	Description	Setting/Contents
rs232OutSigName *(rs232OutSigEntry 2)*	Contains the identification of a hardware output signal.	Supports only the following values: **cts(2)** – Clear To Send **dsr(3)** – Data Set Ready **dcd(6)** – Received Line Signal Detector
rs232OutSigState *(rs232OutSigEntry 3)*	Contains the current signal state.	Supports only the following values: **on(2)** – The signal is asserted **off(3)** – The signal is deasserted
rs232OutSigChanges *(rs232OutSigEntry 4)*	Indicates the number of times that a signal has changed from on to off, or off to on.	Increments the object each time that the signal is sampled (every 100 ms) and the signal state is different from the previous state.

Enterprise MIB Objects

The following lists the Paradyne Enterprise specific MIB Objects supported by the unit.

Device Configuration Variable (pdn-common 7)

The variable devConfigAreaCopy in the devConfigArea group is supported. This variable allows the entire contents of one configuration area to be copied into another configuration area. The unit only supports the following values.

Table C-13. Device Configuration Variable

Object	Description	Setting/Contents
devConfig AreaCopy	A “get” of this object will always return noOp.	**noOp(1)**
	Copy from active area to customer 1 area.	**active-to-customer1(2)**
	Copy from active area to customer 2 area.	**active-to-customer2(3)**
	Copy from customer 1 area to active area.	**customer1-to-active(4)**
	Copy from customer 1 area to customer 2 area.	**customer1-to-customer2(5)**
	Copy from customer 2 area to active area.	**customer2-to-active(6)**
	Copy from customer 2 area to customer 1 area.	**customer2-to-customer1(7)**
	Copy from factory area to active area. There is only one factory area for the unit.	**factory1-to-active(8)**
	Copy from factory area to customer 1 area.	**factory1-to-customer1(9)**
	Copy from factory area to customer 2 area.	**factory1-to-customer2(10)**

Port Usage Table, pdn-devPortUsage (pdn-interfaces 3)

The Port Usage Table specifies whether the Management port is configured for ASCII alarms, as an SNMP management link, or is disabled. Supports the values **alarm(1)**, **netLink(3)**, and **none(5)**.

DDS Interface Specific Definitions, pdn-dds (pdn-interfaces 2)

The DDS Interface Specific Definitions contain objects that are used to manage the DDS Network Interface. Fully supported by the unit.

Device Security, pdn-security (pdn-common 8)

Use the Device Security table to control the number of SNMP managers that may access the unit, as well as the unit access level (read or read/write). Fully supported by the unit.

Device Traps, pdn-traps (pdn-common 9)

Controls the SNMP managers to which the unit reports traps. Fully supported by the unit.

Device Control, pdn-control (pdn-common 10)

Uses the devControlReset object to reset the unit. Fully supported by the unit.

Standards Compliance for SNMP Traps

D

SNMP Traps Overview

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 user interface traps, along with several enterprise-specific traps:

- authenticationFailure
- warmStart
- linkUp
- linkDown

Trap: authentificationFailure

SNMP Trap	Description	Possible Cause
authenticationFailure	Failed attempts to access the unit.	■ SNMP message not properly authenticated. ■ Three unsuccessful attempts were made to enter a correct login/password combination. ■ IP address security is enabled, and a message was received from SNMP manager whose address was not on the list of approved managers. There are no variable-bindings.

Trap: 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.	■ Reset command. ■ Power disruption.

Traps: linkUp and linkDown

The link SNMP traps are:

- **linkUp** – The unit recognizes that one of the failed communication interfaces is operational (up).
- **linkDown** – The unit recognizes a failure in one of the communication interfaces.

The following table describes the conditions that define linkUp and linkDown for each interface:

Interface	linkUp/Down Variable-Bindings	Possible Cause
Physical Sublayer – Represented by the entry in the MIB II Interfaces Table.		
DDS network (Supported by the media-specific DDS Enterprise MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ ifType (RFC 1573) ■ ddsStatus (DDS Enterprise MIB)	■ **linkDown** – One or more alarm conditions are active on the interface. Alarm conditions include: – No Signal – Out of Service – Out of Frame – Crossed Pair Detected – In-band Framing Error – Excessive Bipolar Violations (BPVs) ■ **linkUp** – No alarms on the interface.
Synchronous User Data Port (Supported by the media-specific RS232-Like MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ ifType (RFC 1573)	■ **linkDown** – The Alarm condition active on the interface is DTR Off. The DTR alarm condition only generates a linkUp/linkDown trap if the DTE supports the DTR lead. ■ **linkUp** – No alarm on the interface.

Traps: Enterprise Specific

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

Trap	What It Indicates	Possible Cause
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 or an SNMP manager. 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 user interface or an SNMP manager.
enterpriseTestStop(105)	All tests have been halted.	All tests have been halted on an interface.

There are no variable-bindings for enterpriseSelfTestFail, enterpriseDeviceFail, and enterpriseConfigChange.

The tests that affect the enterpriseTestStart, enterpriseTestStop, and the variable-binding are different for each particular interface. Diagnostic tests are only supported on the physical DDS 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**
Physical Sublayer		
DDS network	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ ifType (RFC 1573) ■ ddsTestType (DDS Enterprise MIB)	■ enterpriseTest Start – Any one of the following tests is active on the interface: – DSU Loopback – CSU Loopback – Send 511 pattern – Monitor 511 pattern ■ enterpriseTest Stop – No longer has any tests running on the interface.
Synchronous User Data Ports	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ ifType (RFC 1573) ■ ifTestType (RFC 1573)	■ enterpriseTest Start – Any one of the following tests is active on the port: – Local Loopback (DTE) – Send 511 pattern – Monitor 511 pattern ■ enterpriseTest Stop – No longer has any tests running on the port.

Cables and Pin Assignments

E

Cabling Overview

The following sections provide pin assignments:

- Terminal Port EIA-232 Connector
- Management Port EIA-232 Connector
- V.35 User Data Port Connector
- Standard EIA-232-D Crossover Cable
- LAN Adapter Converter and Cable
- Modular RJ48S DDS Network Interface Cable

Terminal Port EIA-232 Connector

The Terminal port connects to a PC or VT100-compatible terminal.

Signal	Direction	Pin #
Transmit Data (TXD)	To DSU (In)	2
Received Data (RXD)	From DSU (Out)	3
Request to Send (RTS)	To DSU (In)	4
Clear to Send (CTS)	From DSU (Out)	5
Data Set Ready (DSR)	From DSU (Out)	6
Signal Ground (SG)	—	7
Carrier Detect (CD)	From DSU (Out)	8
Data Terminal Ready (DTR)	To DSU (In)	20

Management Port EIA-232 Connector

The following table shows the signals and pin assignments for the Management port connector.

Signal	Direction	Pin #
Transmit Data (TXD)	To DSU (In)	2
Received Data (RXD)	From DSU (Out)	3
Request to Send (RTS)	To DSU (In)	4
Clear to Send (CTS)	From DSU (Out)	5
Data Set Ready (DSR)	From DSU (Out)	6
Signal Ground (SG)	—	7
Carrier Detect (CD)	From DSU (Out)	8
Transmit Clock (TXC)	From DSU (Out)	15
Received Clock (RXC)	From DSU (Out)	17
Data Terminal Ready (DTR)	To DSU (In)	20
External Tx Clock (XTXC)	To DSU (In)	24

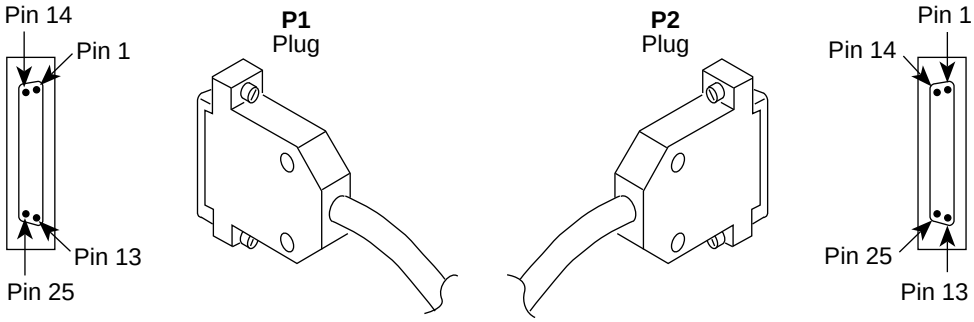
V.35 User Data Port Connector

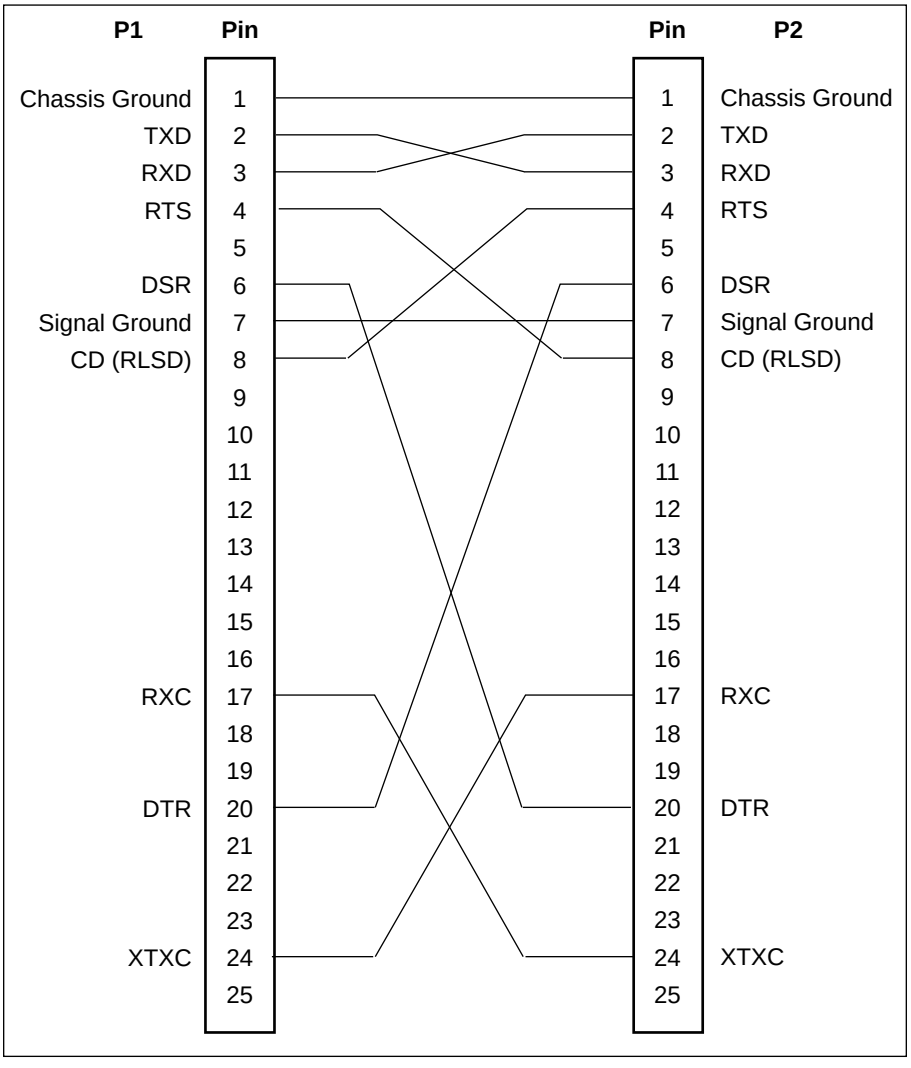
The following table provides the pin assignments for the 34-position V.35 connector to the User Data terminal equipment.

Signal	ITU CT#	Direction	34-Pin Socket Connector
Signal Ground/Common	102	—	B
Request to Send (RTS)	105	To DSU (In)	C
Clear to Send (CTS)	106	From DSU (Out)	D
Data Set Ready (DSR)	107	From DSU (Out)	E
Received Line Signal Detector (RLSD or LSD)	109	From DSU (Out)	F
Data Terminal Ready (DTR)	108/1, /2	To DSU (In)	H
Remote Loopback (RL)	140	To DSU (In)	N
Local Loopback (LL)	141	To DSU (In)	L
Transmitted Data (TXD)	103	To DSU (In)	P (A) S (B)
Received Data (RXD)	104	From DSU (Out)	R (A) T (B)
Transmitter Signal Element Timing — DTE Source (XTXC or TT)	113	To DSU (In)	U (A) W (B)
Receiver Signal Element Timing — DCE Source (RXC)	115	From DSU (Out)	V (A) X (B)
Transmitter Signal Element Timing — DCE Source (TXC)	114	From DSU (Out)	Y (A) AA (B)
Test Mode Indicator (TM)	142	From DSU (Out)	NN

Standard EIA-232-D Crossover Cable

A standard crossover cable can be used to connect either the Terminal port or the Management port to an external modem.



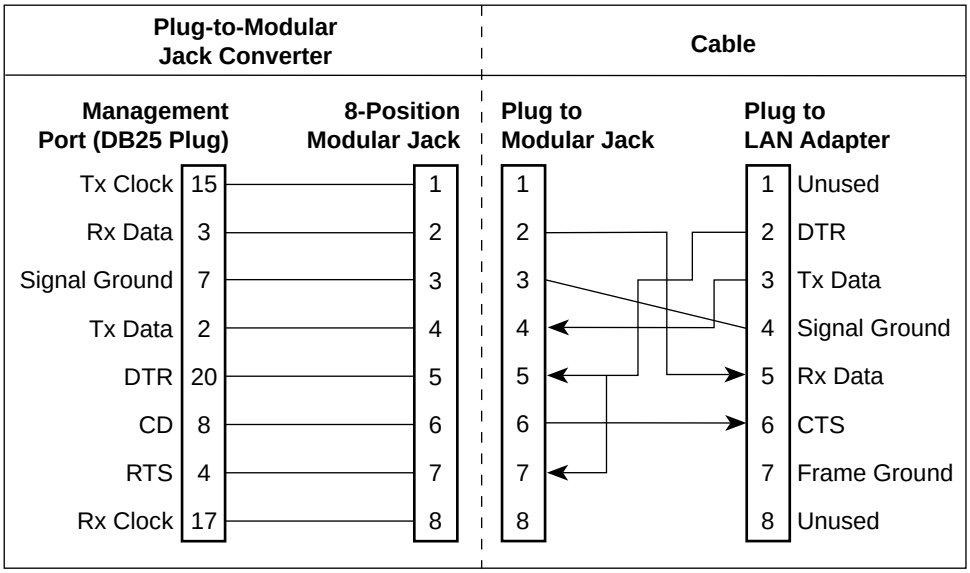


496-15180

LAN Adapter Converter and Cable

The following figure shows the:

- Pin assignments for the DB25 plug to modular jack converter between the Management port and the 8-conductor LAN Adapter cable and
- Pin assignments for the custom 8-conductor cable (with modular plugs on both ends) between the converter and the LAN Adapter.



496-15179

Modular RJ48S DDS Network Interface Cable

Network access is via a 14-foot modular cable with an RJ48S keyed plug connector on each end.

RJ48S DDS Network Interface Cable Functions	Circuit	Pin #
Transmitted data to the local loop	R	1
Transmitted data to the local loop	T	2
Received data from the local loop	T1	7
Received data from the local loop	R1	8

Glossary

agent	A software program housed within a device to provide SNMP functionality. Each SNMP agent stores management information and responds to the manager's request.
aggregate	A single bit stream that combines two or more bit streams.
ASCII	American Standard Code for Information Interchange. A 7-bit code that establishes compatibility between data services. ASCII is the standard for data transmission over telephone lines.
ASCII Terminal or Printer	Devices that can be attached, either locally or remotely, to display or print the DSU's alarm messages.
asynchronous	A data transmission that is synchronized by a transmission start bit at the beginning of a character (five to eight bits) and one or more stop bits at the end.
AT Command Set	Attention Command Set. A group of commands, issued from an asynchronous DTE, that allows control of the modem while in Command mode. All commands must begin with the characters AT and end with a carriage return.
ATI	Asynchronous terminal interface. This feature allows a device to be controlled from an async (asynchronous) terminal like an ASCII (VT100-compatible) terminal.
autobaud mode	An operational mode in which the DSU forces automatic setting of the DDS line rate/speed (56 or 64 kbps) as soon as a valid DDS network signal is detected.
AUX port	The auxiliary communications port on a router.
BPV	Bipolar Violation. A modified bipolar signaling method in which a control code is inserted.
CCA	Circuit Card Assembly. A printed circuit board to which separate components are attached.
CCITT	Consultative Committee on International Telegraphy and Telephony. See ITU.
CD	Carrier Detect. A signal indicating that energy exists on the transmission circuit. Associated with Pin 8 on an EIA-232 interface.
channel	An independent data path.
CMI	Control Mode Idle. A control signal sent over the DDS line to indicate that no data is being sent.
COM port	Communications port. A computer's serial communications port used to transmit to and receive data from a DCE. The DCE connects directly to this port.
configuration option	Device software that sets specific operating parameters for the DSU.
CPE	Customer Premises Equipment. Terminating equipment supplied by either the customer or some other supplier that is connected to the telecommunications network (e.g., DSUs, terminals, phones, routers, modems).
CSU	Channel Service Unit. The function of the DSU that protects the T1 line from damage and regenerates the T1 signal.
CTS	Clear to Send. An EIA-lead standard for V.24 circuit CT 106; an output signal (DCE-to-DTE).

DCE	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.
DDS	Digital Data Service. Provides digital communication circuits.
DMI	Data Mode Idle. Refers to a sequence of ones transmitted or received on the DDS network.
DSR	Data Set Ready. An EIA-lead standard for V.24 circuit CT 107; an output signal (DCE-to-DTE).
DSU	Data Service Unit. Data communications equipment that provides an interface between the DTE and the digital network.
DTE	Data Terminal Equipment. The equipment, such as computers and printers, that provides or creates data.
DTR	Data Terminal Ready. An EIA-lead standard for V.24 circuit CT 108; an input signal (DTE-to-DCE).
EIA	Electronic Industries Association. This organization provides standards for the data communications industry to ensure uniformity of interface between DTEs and DCEs.
EIA-232	The EIA's standards defining the 25-pin interface between the DTE and DCE.
Enterprise MIB	MIB objects unique to Paradyne devices.
excessive BPV	An excessive bipolar violation condition results when at least one invalid bipolar violation has occurred every 20 milliseconds for 2 seconds.
factory defaults	A predetermined set of configuration options for general operation.
FCC	Federal Communications Commission. Board of Commissioners that regulates all U.S. interstate, intrastate, and foreign electrical communication systems that originate from the United States.
frame relay	A switching interface that is designed to get frames from one part of the network to another as quickly as possible.
full-duplex	The capability to transmit in two directions simultaneously.
HDLC	High-Level Data Link Control. A communications protocol defined by the International Standards Organization (ISO).
ICMP	Internet Control Management Protocol. Internet protocol that allows for the generation of error messages, tests packets, and information messages related to IP.
IMC	In-band Management Channel. A proprietary TDM channel used for IP connectivity.
interface	A shared boundary between functional units.
IP	Internet Protocol. The TCP/IP standard protocol that defines the unit of information passed across an Internet and provides the basis for packet delivery service. IP includes the ICMP control and error message protocol as an integral part. The entire protocol suite is often referred to as TCP/IP because TCP and IP are the two most fundamental protocols.
IP address	The IP address has a host component and a network component. The address is assigned to hosts or workstations with direct Internet access to uniquely identify entities on the Internet.
ITU	International Telecommunication Union, formerly known as CCITT. An advisory committee established by the United Nations to recommend communications standards and policies.
LADS	Local Area Data Set is used to provide a point-to-point link between two devices (also called LDM – limited distance modem).

LAN	Local Area Network. A network designed to connect devices over short distances, like within a building.
latching loopback	A latching loopback can only be initiated or terminated by the 64 kbps clear channel network service provider.
LED	Light Emitting Diode. A status indicator that responds to the presence of a certain conditions.
link layer protocol	The protocol that regulates the communication between two network nodes.
LL	Local Loopback. An EIA-lead standard for V.24 circuit CT 141; an input signal (DTE-to-DCE).
loopback	Used to test various portions of a data link in order to isolate an equipment or data line problem. A diagnostic procedure that sends a test message back to its origination point.
LSD	Line Signal Detect. An EIA-lead standard for V.24 circuit CT 109; an output signal (DCE-to-DTE).
manager (SNMP)	The device that queries agents for management information, or receives unsolicited SNMP trap messages indicating the occurrence of specific events.
MIB	Management Information Base. The set of variables a device running SNMP maintains. Standard, minimal MIBs have been defined, and vendors often have private enterprise MIBs. In theory, any SNMP manager can talk to any SNMP agent with a properly defined MIB. MIB-II refers to an extended management database that contains variables not defined in the original MIB I.
multiplexing	A method for interleaving several access channels onto a single circuit for transmission over the network.
NMS	Network Management System. A computer system used for monitoring and controlling network devices.
node	A connection or switching point on the network.
non-latching loopback	A non-latching loopback can only be initiated or terminated by the 56 kbps network service provider.
NS	No Signal. A network-reported condition.
object (SNMP)	A specific item within the Management Information Base (MIB).
OOF	Out Of Frame. An error condition in which frame synchronization bits are in error. A network-reported condition.
OOS	Out of Service. A digital network trouble signal.
PAD	Packet Assembler/Diassembler.
point-to-point circuit	A data network circuit with one control and one tributary device.
PPP	Point-to-Point Protocol. A link-layer protocol used by SNMP.
protocol	The rules that govern how devices exchange information on a network. It covers timing, format, error control, and flow control during data transmission.
PSTN	Public Switched Telephone Network. A network shared among many users who can use telephones to establish connections between two points.
reset	A reinitialization of the device that occurs at power-up or in response to a reset command.
RFC	Request for Comments. The set of documents that describes the standard specifications for the TCP/IP protocol suite.

RIP Routing Information Protocol. Specifies the routing protocol used between DSUs.

RLSD Receive Line Signal Detect. See CD.

router A device that makes decisions about the paths network traffic should take and forwards that traffic to its destination. A router helps achieve interoperability and connectivity between different vendor's equipment, regardless of protocols used.

RS-232 An EIA standard for the 25-pin DCE/DTE interface. Same as EIA-232.

RTS Request to Send. An EIA-lead standard for V.24 circuit CT 105; an input signal (DTE-to-DCE).

RXC Received Clock. An EIA-lead standard for V.24 circuit CT 115; an output signal (DCE-to-DTE).

RXD Received Data. An EIA-lead standard for V.24 circuit CT 104; an output signal (DCE-to-DTE).

SDLC Synchronous Data Link Control. A standard data link protocol.

SLIP Serial Line Internet Protocol. A link layer protocol being used over serial lines by IP.

SNMP Simple Network Management Protocol. A generic internet network management protocol that allows the device to be managed by any industry-standard SNMP manager.

subnet An IP addressing standard in which a portion of the host address can be used to create multiple network addresses that are logically a subdivision of the network address.

subnet address The subnet portion of an IP address. In a subnetted network, the host portion of an IP address is split into a subnet portion and a host portion using a subnet address mask. This allows a site to use a single IP network address for multiple physical networks.

subnet mask An integer used with the IP address of the host to determine which bits in the host address are used in the subnet address.

synchronous Data transmission that is synchronized by timing signals. Characters are sent at a fixed rate.

TCP/IP Transmission Control Protocol/Internet Protocol. Refer to IP.

TDM Time Division Multiplexer. A device that enables the simultaneous transmission of multiple independent data streams into a single high-speed data stream.

Telnet 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 the user for that host.

TM Test Mode. An EIA-lead standard for V.24 circuit CT 142; an output signal (DCE-to-DTE).

TXC Transmit Clock. An EIA-lead standard for V.24 circuit CT 114; an output signal (DCE-to-DTE).

TXD Transmit Data. An EIA-lead standard for V.24 circuit CT 103; an input signal (DTE-to-DCE).

UDP User Datagram Protocol. An Internet protocol.

V.35 ITU-T standard for a high-speed, 34-pin, DCE/DTE interface.

WAN Wide Area Network. A network that operates over long distances and spans a relatively large geographic area (e.g., a country).

Index

Numbers

A

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W