

DataSMART[®] T3/E3 IDSU

User's Guide

Document #5000164



Copyright

© 1994-1996, 2001 by Kentrox, LLC. All Rights Reserved.
Printed in the U.S.A.

Specifications published here are current or planned as of the date of publication of this document. Because we are continuously improving and adding features to our products, Kentrox reserves the right to change specifications without prior notice. You may verify product specifications by contacting our office.

In no event shall Kentrox be liable for any damages resulting from loss of data, loss of use, or loss of profits. Kentrox further disclaims any and all liability for indirect, incidental, special, consequential or other similar damages. This disclaimer of liability applies to all products, publications and services during and after the warranty period.

Trademark information

Kentrox, DataSMART, and T-SMART are registered trademarks of Kentrox, LLC. MultiSMART is a trademark of Kentrox, LLC.

All other product names are trademarks or registered trademarks of their respective owners.

Revision history

Part #	Date	Description
65-15951103	November 1996	Issue 3
5000164	December 2001	Issue 4

Contents

	Preface	7
Chapter 1	Introduction	
	Typical applications	10
	Scalable multi-rate bandwidth and programmable interfaces	10
	Alarm dial-out	11
	Key features of the DataSMART T3/E3 IDSU	12
	T3 or E3 network access	12
	Scalable multi-rate bandwidth and programmable data ports	12
	Telnet and embedded SNMP via SLIP	12
	T3/E3 line diagnostics	12
	End-to-end performance monitoring	12
	Alarm dial-out	12
	Nonvolatile memory	12
	Using the DataSMART T3/E3 IDSU	13
	Using the command-line interface	13
	Logging in	15
	Through the control port: stand-alone	15
	Through the control port: daisy-chained	15
	Telnet access	15
	Logging out	16
Chapter 2	Establishing system security	
	Securing the command-line interface	18
	Restricting access	18
	Adding a password	19
	Deleting a password	19
	Viewing the current passwords	20
	Logging in with a password	21
	Entering a password	21
	Viewing a password's access level	21
	Determining if passwords have been set for the unit	22

Chapter 3 **Configuring the system**

Specifying system parameters	24
Viewing the current settings	24
Setting date and time	25
Naming the device	26
Enabling/disabling the front-panel	26
Selecting the control port for alarm or trap outputs	27
Specifying the system clock	28
Zeroing all counters	29
Obtaining product version information	29
Resetting to default values	30
Configuring the control port	31
Viewing the current configuration	31
Enabling/disabling character echo	31
Configuring alarms	32
Viewing the current configuration	33
Enabling/disabling the alarm relay connector	34
Enabling/disabling alarm messages	34
Formatting the alarm messages (ASCII or numeric)	35
Enabling alarm dial-out	35
Programming the dial-out string	36
Enabling/disabling alarms on incoming yellow (or RAI)	36
Enabling/disabling alarms on AIS	36
Setting the threshold for errored seconds (ES)	37
Setting the threshold for unavailable seconds (UAS)	37

Chapter 4 **Configuring interfaces**

Configuring the network interface	40
Viewing the current network interface configuration	40
Specifying NI framing format	41
Setting the output level of the transmit signal	44
Specifying transmit line build-out attenuation	44
Configuring the data port	45
Viewing the current data port configuration	46
Setting the transmit and receive clock rate	47
Specifying the physical interface	48
Enabling/disabling payload scrambling	48

Chapter 5 Performance monitoring

Accessing reports	50
Controlling page length	50
Clearing the performance database	51
Interpreting the User NI report	52
Time intervals in the short report	52
Time intervals in the long report	53
Performance measurements	54
Interpreting the Far-end report (available only for T3 C-Bit framing)	55
Interpreting the Subrate Data Performance report	56
Interpreting the Statistical reports	57
Interpreting the Alarm History report	58

Chapter 6 Troubleshooting

Interpreting the front-panel LEDs	60
Monitoring alarm messages	63
Examining system status	64
Troubleshooting tree	66
EQF	66
NI LOS	66
NI OOF	67
NI AIS	67
NI YEL	67
NI EER	68
DP NSYN	68
Running the self-test diagnostics	69
Using the network signal monitor jacks	70
Using loopbacks	71
Line loopback	71
Payload loopback	71
Local loopback	72
Data terminal loopback	73
Setting and resetting loopbacks in your local device	74
Setting and resetting loopbacks remotely (T3 C-Bit framing only)	75

Chapter 7	Using Telnet and SNMP	
	Enabling SLIP and specifying local IP information	78
	Viewing the current settings	78
	Setting the IP address and subnet mask	79
	Enabling/disabling SLIP	79
	Setting the default router	80
	Setting the Telnet password	80
	Specifying the SNMP configuration	81
	Viewing the current settings	81
	Setting SNMP community strings	83
	Configuring SNMP trap hosts	84
	Enabling/disabling the SNMP agent	84
	Specifying source address screening configuration	85
	Viewing the current settings	85
	Enabling/disabling address screening	86
	Adding a host to the address screening list	86
	Deleting a host from the address screening lists	86
	Traps & MIBs	87
Chapter 8	Quick Reference	
	Command-line menus and commands	90
	Front-panel thumbwheel switch	96
	Specifications	98
	MIB II (RFC 1213) support	104
	DS3/E3 MIB (RFC 1407) support	120
	Glossary	131
	Index	137

Preface

This manual is the comprehensive reference source for operation of the ADC Kentrox DataSMART T3/E3 Intelligent Data Service Unit (IDSU). It provides specific information for configuring the DataSMART T3/E3 IDSU, along with detailed listings of all menus, commands, and product specifications.

Who should read this manual?

This manual is intended as a reference source for ongoing operation of the DataSMART T3/E3 IDSU. It covers all possible operations and configuration choices in detail. For initial installation, power-up, and basic configuration of the unit, we recommend that you first turn to the *DataSMART T3/E3 IDSU Installation Guide*.

Viewing this manual as a PDF file

This manual is designed to be used as both a printed book and a PDF file, and includes the following features for PDF viewing:

- Cross-references are clickable hyperlinks that appear in blue text.
- Chapters and section headings are represented as clickable bookmarks in the left-hand pane of the Acrobat viewer.
- Page numbering is consistent between the printed page and the PDF file to help you easily select a range of pages for printing.

You can obtain PDF files of our manuals by visiting <http://www.kentrox.com>.

Related publications

In addition to this manual, you will have received:

- *DataSMART T3/E3 ISDU Installation Guide*

About this manual

This manual contains the following information:

“Preface” (this section) explains the purpose, organization, and conventions used in this manual and tells how to contact ADC Kentrox Technical Support if you should run into difficulties.

“Introduction” describes the applications and features of the DataSMART T3/E3 IDSU. It also introduces you to the IDSU commands.

“Establishing system security” shows how to set passwords for the DataSMART T3/E3 IDSU unit.

“Configuring the system” describes in detail all of the system-level configuration choices you can make. This includes setting up the system source clock, configuring the alarm formats and output, and configuring the DCE and DTE control ports.

“Configuring interfaces” describes in detail all the configuration choices available for setting up the network interface and the data port.

“Performance monitoring” shows you how to access and use the DataSMART T3/E3 ISDU performance reports and the Alarm History report.

“Troubleshooting” shows you how to use the features of the DataSMART T3/E3 ISDU to recognize and troubleshoot abnormal conditions. It describes use of the ISDU front-panel LEDs, alarm messages, and diagnostic tools.

“Using network management” shows you how to set up and use the DataSMART T3/E3 ISDU in a network management environment. It describes the SLIP interface and shows how to establish a Telnet link. It also shows how to access the embedded MIB objects via an SNMP network management tool.

“Quick reference” summarizes DataSMART T3/E3 ISDU menus and commands. It also provides a listing of product specifications, and a listing of the embedded MIB objects.

At the back of the manual, you’ll also find a glossary of terms and an index.

Conventions used in this manual

This manual employs the following conventions when explaining command-line syntax:

Literals	Bold type identifies commands and syntax elements that must be entered exactly as shown in the text.
<i>Variables</i>	Italic type identifies variable syntax elements, such as values or alphanumeric strings you can enter.
<i>x/y</i>	A vertical line between elements means that the elements are mutually exclusive; you can select one and only one of the elements.
[]	Brackets indicate items that are optional.

Who to call for assistance

If you need assistance with this product or have questions not answered by this manual, please visit our Support page on the Kentrox Web site. You are also welcome to call or send email to our Technical Assistance Center. Please have your product’s software revision and hardware serial numbers available to give to the Support representative. All product returns must include a Return Authorization number, which you can obtain by calling the Technical Assistance Center.

The numbers listed below are current at the time of publication. See the Kentrox Web site for detailed contact and warranty information.

1-800-733-5511 (continental USA only)

1-503-350-6001

email: support@kentrox.com

<http://www.kentrox.com>

1

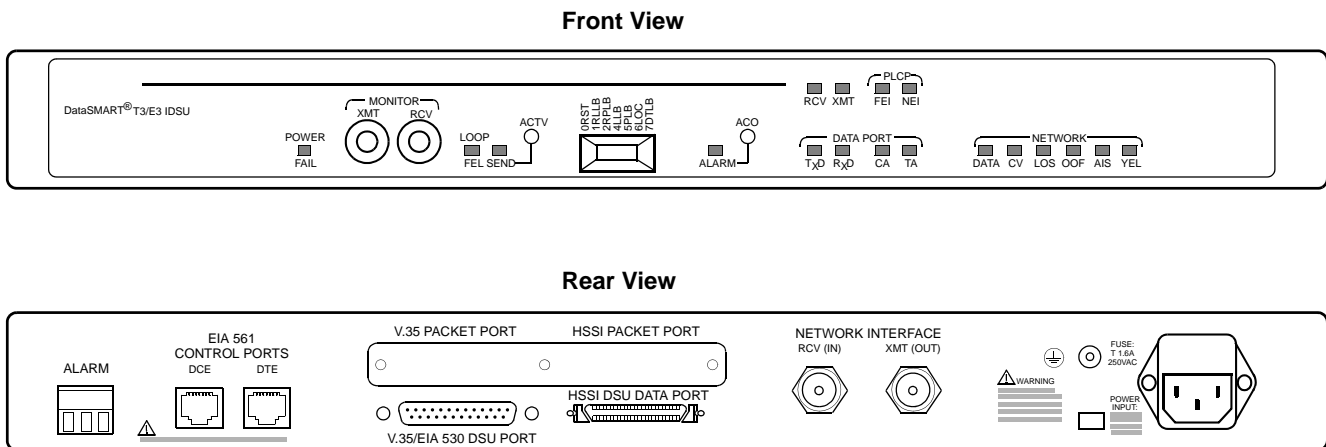
Introduction

The DataSMART T3/E3 IDSU is an intelligent data service unit (IDSU) for direct connection between T3 and E3 circuits and data terminal equipment (DTE).

The DataSMART T3/E3 IDSU supports high-speed synchronous transmission rates up to 45 MHz for T3, and up to 34 MHz for E3. Its transmission rate is scalable to support different multi-rate applications. This feature, coupled with a variety of data port interfaces (HSSI, V.35, EIA-530), allows you to use the IDSU with high- or lower-speed routers, channel extenders, and other devices, for applications such as LAN-to-LAN communications, CAD/CAM systems and host-to-workstation communications.

The IDSU comes in either an AC- or a DC-powered model. Both models are housed in the same one-unit-high (1U) rack-mount box.

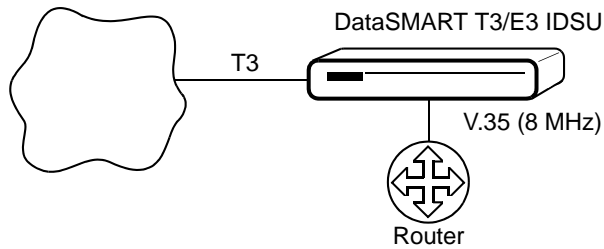
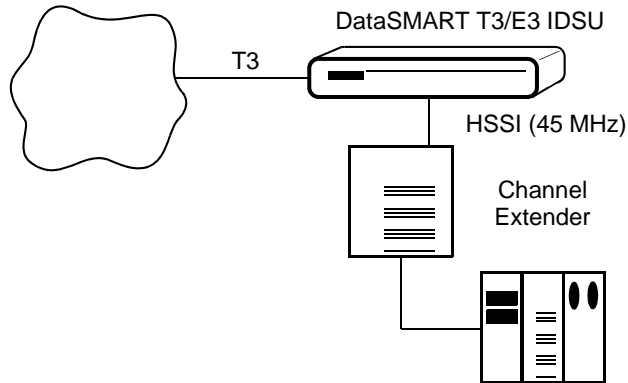
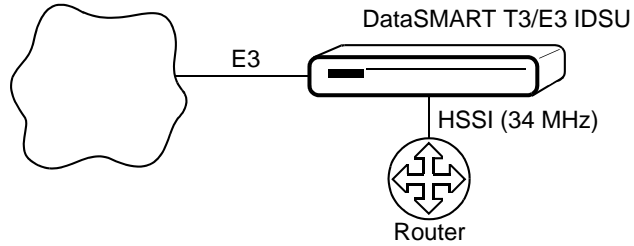
Figure 1—The DataSMART T3/E3 IDSU



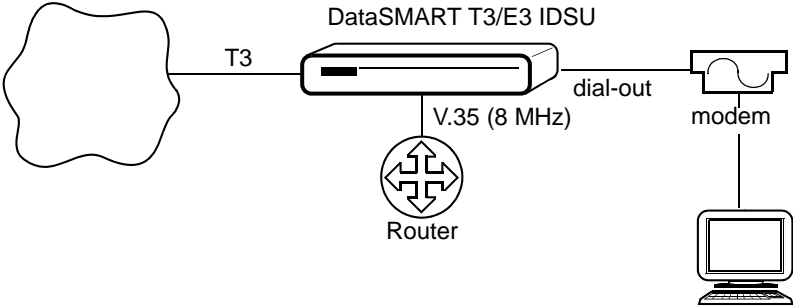
Typical applications

The DataSMART T3/E3 IDSU supports many applications for direction connection of a DTE to the T3 or E3 circuit.

Scalable multi-rate bandwidth and programmable interfaces



Alarm dial-out



Key features of the DataSMART T3/E3 IDSU

T3 or E3 network access

The DataSMART T3/E3 IDSU supports T3 M13 or C-bit parity, or E3 CCITT G.751 standard framing.

Scalable multi-rate bandwidth and programmable data ports

The DataSMART T3/E3 IDSU connects a wide variety of data terminal equipment to the T3 or E3 circuit. It provides a high-speed HSSI port for data transmission rates up to 45 MHz for T3, and up to 34 MHz for E3. It also provides a user-programmable V.35/EIA-530 data port for transmission rates up to 8 MHz for T3 or E3. Adapters are available for connecting the port to EIA-449, X.21, or V.35.

Transmission rates are scalable in 0.5 MHz increments, starting at 0.05 MHz, giving you support for partial or full T3/E3 service.

Telnet and embedded SNMP via SLIP

The DataSMART T3/E3 IDSU allows a SLIP interface via its control port. Through this interface, you can Telnet to the IDSU and access its entire user-interface command set.

The IDSU also allows an SNMP manager to access (set or get) embedded MIB objects via the SLIP interface. The embedded MIBs are a subset of the standard MIB II and DS3/E3 MIBs (see [Chapter 7](#), starting on [page 77](#)). The IDSU supports link-up, link-down, and cold-start traps.

T3/E3 line diagnostics

The DataSMART T3/E3 IDSU offers a complete suite of diagnostic tools, including:

- LEDs for alerting you to problems on lines at the network interface and data port
- Alarm messages and SNMP traps
- Loopbacks that can be set remotely or locally

End-to-end performance monitoring

The DataSMART T3/E3 IDSU has extensive non-intrusive reports that show the performance of the T3/E3 line. With these reports, you can see the quality of the signal over a period of time and recognize problems before the service goes down.

The performance monitoring reports show the signal quality for the previous 24 hours in 15-minute increments. All reports are detailed, including information on various types of error counts and alarm states. They are easy to read and can be formatted for printable files or screen displays.

Alarm dial-out

The DataSMART T3/E3 IDSU outputs alarms as ASCII messages. If you want the IDSU to notify a remote workstation of a pending alarm before sending the message, you can set up an alarm dial-out table. Alarms are also output as traps through a SLIP interface.

Nonvolatile memory

The DataSMART T3/E3 IDSU configuration is stored in nonvolatile memory, so the unit can retain its configuration for a minimum of 500 days without power.

Using the DataSMART T3/E3 IDSU

Using the command-line interface

With the command-line interface you use a terminal (or a PC running terminal emulator software) to manage and monitor the DataSMART T3/E3 IDSU.

To help you find your way through the interface, the IDSU uses “menus” that might be more properly thought of as help displays.

Each command is categorized and placed in a menu. For instance, all the commands for generating reports are in the Reports menu. To see the list of all menus as shown in the following figure, enter **MM**.

```
DataSMART T3/E3 IDSU Version 3.22 Copyright (c) 1992-1995 Kentrox
      ADDRESS: 00:00:000      NAME: PORTLAND,OR

MM          - Main Menu
SS          - Status Menu
R           - Performance Report Menu
PE          - Password Entry Menu

LM          - Local Maintenance Menu
RM          - Remote Maintenance Menu

AC          - Alarm Configuration Menu
CC          - Control Port Configuration Menu
NC          - NI Configuration Menu
PC          - Password Configuration Menu
SC          - System Configuration Menu
TCP        - TCP/IP Configuration Menu
SNMP       - SNMP Configuration Menu
SCREEN     - Source Address Screening

^D          - Logout
^D<xx>:<yy>:<zzz>^E - Address Another Unit

MM>
```

To see one of the menus, enter the menu name at the prompt. For instance, to see the Reports menu, enter **R** at the prompt.

```
PERFORMANCE REPORT MENU

UNSR / UNLR - User NI Short/Long Performance Report
FESR / FELR - Far End PRM Data Short/Long Performance Report
SDLR        - Subrate Data Long Performance Report

NSR         - User NI Statistical Report
AHR         - Alarm History Report

PL:<n>      - Page Length, n = 20, 70, (P - Page Break) (V - View)

R >
```

Each time you change menus the command-line prompt changes to indicate which menu is current. In the preceding figure, the first line shows a prompt of “MM>” meaning that the Main menu is current. However, once R is entered and the Reports menu is displayed, the prompt becomes “R>,” indicating that the Reports menu is current.

The current menu displays when you press the Enter key. In normal use you are likely to use a series of commands from a given menu, and so you can make that menu current and get a menu listing whenever you need it by pressing the Enter key. However, you may enter any command at the command line, even if it is not on the “current” menu.

Command-line syntax

A typical command line consists of the command and zero or more arguments, all separated by one or more delimiters. The syntax and acceptable delimiters for each command are described under the individual command entries in this manual. The delimiters are required.

Type-ahead

You may enter the next command while a previous command is executing. The maximum type-ahead is three commands or 256 characters, whichever is less.

Logging in

In general, a password is not needed to log into a DataSMART T3/E3 IDSU. Though the IDSU supports passwords, the passwords do not prevent login but instead restrict users from executing various commands. (See Chapter 2 for procedures on setting passwords.)

Depending on whether the DataSMART T3/E3 IDSU is daisy-chained or is stand-alone, the procedure for logging in differs.

Through the control port: stand-alone

On a stand-alone unit, the device has an address of 00:00:000. In this case, simply push the Enter key to log in. The IDSU will display the Main menu, and then the command prompt, indicating you are logged in.

Through the control port: daisy-chained

With daisy-chained units, each unit in the daisy chain has an address. To log into an IDSU that is daisy-chained, enter this:

```
<Ctrl-D>xx:yy:zzz<Ctrl-E>
```

where *xx:yy:zzz* is the address of the unit you want to log into. Note that the colon delimiters are required.

Telnet access

You can log into the IDSU using Telnet over a SLIP interface through the control port. When you attempt to log in, you will be prompted for a Telnet password. You must assign a Telnet password to the IDSU before you attempt to access it via Telnet. If the IDSU has not been assigned a Telnet password, you will not be able to log in.

See [Chapter 7](#), starting on [page 77](#), for information on configuring a DataSMART T3/E3 IDSU for Telnet login.

Logging out

You should always log out of the DataSMART T3/E3 IDSU when you are done.

To log out, enter <Ctrl-D>.

You can also log out by disconnecting the control port cable.

The IDSU has an auto-logout feature, that will log you out after a 15-minute period of inactivity.

2

Establishing system security

The DataSMART T3/E3 IDSU can be accessed through an SNMP network manager or through the command-line interface, using either a terminal or Telnet. In order to prevent unauthorized users from changing the system configuration, setting loopbacks, or performing other operations that might disrupt service, you must secure each of these interfaces.

This chapter tells how to secure the command-line interface.

For information about securing SNMP access with community strings, refer to “Setting SNMP community strings” on page 83.

Securing the command-line interface

Security for the command-line interface is achieved through a system of passwords and privilege levels. Any user can access the command line without entering a password. But in order to gain a specific privilege level, the user must enter a password that has that privilege level assigned to it.

Restricting access

By default, there are no restrictions on which commands you can run on the DataSMART T3/E3 IDSU. Every user has super-user privileges. In order to restrict access, you must create at least one password with the super-user privilege level. Once you do, every user is restricted to the read-only privilege level unless they enter a password that permits more extensive privileges. You may create up to ten passwords (assuming you have super-user privileges) and assign them any privilege level you like.

 **NOTE**

The first password you create must be assigned super-user privileges. The unit will not allow you to create lower-level passwords that would lock out higher-level features until those features are accessible to a super-user.

Table 1—Privilege levels

Privilege level	Description
Read-only	Users with no password, and thus no privilege level, have read-only access. They can view menus, status screens, and performance reports, but they cannot execute any diagnostics nor change any configuration options.
Maintenance	Users with this privilege level can execute diagnostic tests and loopbacks. Their activities can potentially disrupt data traffic through the device.
Configuration	Users with this privilege level can execute all tests allowed at the Maintenance level, plus they can change the configuration options of the DataSMART T3/E3 IDSU. Their activities can potentially disrupt service to the device.
Super-user	Users with this privilege level have access to all commands allowed at the Configuration level, plus they have access to the commands that set up and control passwords.

Using Telnet

If you are using Telnet, you must set up a Telnet password, which is independent of the command-line passwords described here. See “Setting the Telnet password” on page 80.

The commands available for setting up and controlling command-line passwords are listed

in the Password Configuration menu. To display this menu, enter **PC** at the command line.

```

                                PASSWORD CONFIGURATION MENU

APS:<access>:<password> - Add Password
                        access   = SA - Super User
                                CA - Configuration
                                MA - Maintenance
                        password = 6 to 12 characters

DPS:<password>         - Delete Password

PCV                    - View Password Configuration

PC>
```

Adding a password

You create a new password by using the **APS** command. You must have super-user privileges. The command syntax is:

APS:*access:password*

access Specify the privilege level you want linked to the password: **SA** (super user), **CA** (configuration), or **MA** (maintenance).

password Specify the password you want added. The string can comprise from six to twelve ASCII printable characters. If the string you enter is either too long or too short, you'll get an error message. Passwords are not case-sensitive. Trailing spaces are not allowed.

Up to ten passwords are allowed. If you attempt to enter an eleventh password, you will get an error message. To add another password, you must first delete an existing password.

Each password must be unique.

New passwords do not take effect until you logout, then log back into the system.

Deleting a password

You delete a password using the **DPS** command. You must have super-user privileges. The command syntax is:

DPS:*password*

password Specify the password you want deleted. The string must match the password exactly, except for case. You can also enter the * wild-card character to delete all current passwords.

NOTE

*All existing passwords are deleted if you reset the unit, either by entering the **RSD** command or by pressing the **ACTV** and **ACO** push-buttons.*

Viewing the current passwords

You can view a listing of current passwords and their privilege levels using the **PCV** command. You must have super-user privileges.

An example listing is shown below. The left column lists the current passwords, the right column identifies the access privilege levels.

```
View Password Configuration

Password      Access
-----      -
WILLIAMS     MA
PARKER       CA
BROWNC       CA
MITCHELL     SA

PC>
```

Logging in with a password

You gain the privilege level associated with a password by entering that password once you have logged into the unit. The commands for entering a password and viewing its access privileges are listed in the Password Entry menu (enter **PE** at the prompt).

```
PASSWORD ENTRY MENU

EPS:<password> - Enter Password
                password = 6 to 12 characters

PEV           - View Access Privileges
PUV           - View User Access Privilege

PE>
```

Entering a password

To gain the privilege level associated with a password, use the **EPS** command. No special privileges are required. The command syntax is:

EPS:*password*

password Enter the password. Passwords are not case-sensitive.

If you enter the password correctly, the DataSMART T3/E3 IDSU responds with the message **PASSWORD ACCEPTED**. If you enter an incorrect password, it responds with the message **PASSWORD DENIED**.

Viewing a password's access level

If you are logged into the device, you can view your privilege level by using the **PUV** command. You do not need any special privilege level. You will receive one of the following messages:

- “User has No Access Privileges” (read-only)
- “User has MA Access Privileges” (maintenance)
- “User has CA Access Privileges” (configuration)
- “User has SA Access Privileges” (super user)

If your password was modified during your current session (e.g., a super-user deleted your password, then added it back with a different privilege level), the change will not become effective until the next time you specify the password with the **EPS** command.

Determining if passwords have been set for the unit

You can learn if passwords have been established for the unit by using the **PEV** command. When you enter this command, the system responds with a display similar to the one shown below. This display tells you a super-user has been established, which means passwords have been set.

You do not need any special privileges to use this command.

```
Password exists for:  
SuperUser      : Yes  
Configuration: Yes  
Maintenance    : Yes  
  
PE>
```

3

Configuring the system

This chapter discusses the commands and options available for programming the DataSMART T3/E3 ISDU system-level parameters, including:

- Setting the unit's time and date
- Specifying the unit's system source clock
- Enabling or disabling the front-panel controls
- Resetting the device to the factory default state
- Configuring the control port
- Configuring alarm message output and format

For information on configuring the unit's network interface and data port, see [Chapter 4](#) on [page 39](#).

For information on configuring the unit for network management, see [Chapter 7](#) on [page 77](#).

Specifying system parameters

Many of the commands for configuring the system parameters are listed in the System Configuration menu. To display this menu, enter **SC** at the system prompt.



NOTE

The System Configuration menu also lists commands for configuring the data port. These commands are described in [Chapter 4](#).

SYSTEM CONFIGURATION MENU

```
SD:<mmm>,<dd>,<yy>    - Set Date
ST:<hh>:<mm>          - Set Time
SN:<id>               - Set Name
SA:<xx>:<yy>:<zzz>    - Set the Unit's Address to slot:shelf:group
EFP / DFP            - Enable/Disable Front Panel Operation
DCE / DTE            - DCE/DTE is the Alarm Output Port
CLK:<src>             - Clock Source, src = I (Internal), L (Looped)
DSUCLK:<xx.x>,<yy.y> - Sets DSU data port clock (direction is NI)
                    xx.x = transmit, yy.y = receive
HSSI / V35 / EIA530 - Select data port as HSSI, V.35 or EIA-530
ESCRAM/DSCRAM        - Enable/Disable Scrambling on the DSU Data Port
ZALL                 - Zero All Counters used in User Reports
WYV                  - What's Your Version
RSD                  - Reset Unit to Dip Switch Defaults
SCV                  - View System Configuration

SC>
```

These commands program the data port. They are covered in [Chapter 4](#).

Viewing the current settings

Before changing any of the system parameters listed in the System Configuration menu, you may want to look at the current settings. You do this by executing the **SCV** command. This command displays the View System Configuration screen.

View System Configuration

```
Date          Time   Name          Address
-----
JAN 14, 1990  20:37  PORTLAND,OR   00:00:000

Timing        Front Panel  Port  Data Port  Transmit  Receive
-----
Looped        Enabled     DCE   HSSI       45.0 MHz  45.0 MHz

Scrambling
-----
Disabled

SC>
```

Field

Description

Date	This field displays the current date setting of the unit.
Time	This field displays the current time setting of the unit.

Field	Description
Name	This field displays the name assigned to the unit you are logged into. The name appears in the Main menu, in all performance reports, and in alarm messages. It is also the name returned for the <i>sysName</i> MIB object.
Address	This field displays the daisy-chain address of the unit you are logged into. The address is in the form of <i>xx:yy:zzz</i> . A value of 00.00.000 identifies a stand-alone unit.
Timing	This field identifies the clock source you have assigned to be used as the system clock. The source is either a timing signal “looped” from the network or the IDSU’s internal clock signal.
Front Panel	This field tells you whether the front-panel thumbwheel switch is enabled or disabled. When disabled, the thumbwheel switch cannot be used to set or reset loopbacks; loopbacks can only be set or reset via the command-line interface.
Port	This field identifies the control port being used for transmitting alarm messages, unless SLIP is enabled. If SLIP is enabled, this field specifies which control port is the SLIP interface.
Data Port	This field identifies the physical data port being used.
Transmit Clock	This field identifies the clock rate used for clocking data input at the data port (transmit data from the DTE).
Receive Clock	This field identifies the clock rate used for clocking data output at the data port (receive data from the network).
Scrambling	This field tells you whether or not payload scrambling is enabled at the data port.

Setting date and time

The DataSMART T3/E3 IDSU uses an internal, real-time clock to time stamp event occurrences. The time stamps appear in alarm messages and performance reports as an aid to troubleshooting. To make the time stamps meaningful, you must set the date and time of the real-time clock upon system installation.



CAUTION!

When you change the date or time parameters of the real-time clock, all performance data is cleared from the performance reports.

You set the date by using the **SD** command. You must have super-user or configuration privileges. The command syntax is:

SD:mmm,dd,yy

mmm Specify the month. You can enter the three-letter abbreviation or the number of the month.

dd Specify the day of the month. The DataSMART T3/E3 IDSU performs a range check on the entered value to see if the day is valid for the given month and year.

yy Specify the last two digits of the year. (00 is year 2,000.)

TIP

If you need to track between Daylight Savings Time and Standard Time, you will need to reset the “time” parameter when local time changes.

You set the time by using the **ST** command. You must have super-user or configuration privileges. The command syntax is:

ST:hh,mm

hh Specify the hour. The time is specified in “24-hour” format, where 12:00 is noon and 00:00 is midnight. Allowed values are 0 to 23, inclusive.

mm Specify the minutes. Allowed values are 0 to 59, inclusive.

Naming the device

Each DataSMART T3/E3 IDSU is assigned a device name that appears in alarm messages, performance reports, and at the top of the Main menu. You can specify any name up to 20 characters long. Usually you specify a name that represents your site or the service you are connected to.

The device name specified here is also the name returned with the *sysName* MIB object.

The default device name is “PORTLAND, OR.”

You change the device name by using the **SN** command. You must have super-user or configuration privileges. The command syntax is:

SN:id

id Enter the device name. The name can be up to 20 characters long, including spaces, commas, or colons. A space, comma, or colon may not appear in the first position. Trailing spaces are truncated.

Enabling/disabling the front-panel

The front-panel of the unit contains a thumbwheel switch you can use to set and reset loopbacks. If you want to secure the front-panel so that you can only set and reset loopbacks from the command-line interface, you can disable the front-panel switch so that a user at the site of the unit cannot inadvertently disrupt service by initiating a loopback.

To enable or disable the front-panel switch, use the following commands. You must have super-user or configuration privileges.

EFP Enable the front-panel control

DFP Disable the front-panel control

These commands do not disable your ability to use the front panel to reset the unit to its factory default settings. You can always reset the unit to defaults.

For information about using the front-panel switch, see [“Front-panel thumbwheel switch” on page 96](#).

Selecting the control port for alarm or trap outputs

When you specify either **DCE** or **DTE**, you are telling the DataSMART T3/E3 IDSU which physical control port to use for the alarm or trap output.

The default setting is DCE.

The setting is stored in the permanent nonvolatile configuration database.

You must have super-user or configuration privileges to change the setting.

Alarm messages

The command-line interface generates unsolicited messages when alarms occur and sends these messages to the control port you specify.

For most applications, you want the IDSU to output alarm messages to the same control port from which it is receiving commands. For example, if you have a control device connected to the IDSU's DCE port, you want alarm messages to go to the DCE port. If you are communicating to the IDSU via a modem, the modem will be connected to the DTE port and alarm messages should go to the DTE port.

If you are using daisy-chained units, alarm messages *must* go to the same control port being used by the control device. The nature of daisy-chaining forces the IDSU to accept commands and to output messages via the same port.

The only time you might want alarm messages to go to a port different than the one being used by the control device is when you are using alarm dial-out. For example, you might want the alarm dial-out to go an external alarm device instead of to the control device. With alarm dial-out, alarm messages must be sent to DTE; the control device can be connected to either DTE or DCE.

Alarm dial-out is disabled in daisy-chained units.

See [page 35](#) for procedures on enabling alarm dial-out.

SLIP and traps

If you are using SLIP, the **DCE** or **DTE** command tells the DataSMART T3/E3 IDSU which control port to use as the SLIP interface. The IDSU expects to receive sets and gets via this interface, and sends traps out this interface.

Daisy-chaining is not allowed with a SLIP interface.

Specifying the system clock

The DataSMART T3/E3 IDSU uses one clock source to time outputs at the network interface and the data port. This clock source is retrieved from the network receive signal when the service provider supplies timing; otherwise, it is derived from the IDSU's internal oscillator.

The default is for the IDSU to retrieve its timing signal from the network receive signal. This is called "looped" timing and is the most common setup. Always use this setting if the service provider supplies timing, because for a T3 or E3 circuit to synchronize properly there must be one and only one timing source for the circuit.

If your service provider does not supply timing, use the IDSU's internal oscillator as the timing source.

NOTE

When set to looped timing, the DataSMART T3/E3 IDSU will default to its internal clock if the clock in the network receive signal is lost.

Use the **CLK** command to specify the timing source. You must have super-user or configuration privileges. The command syntax is:

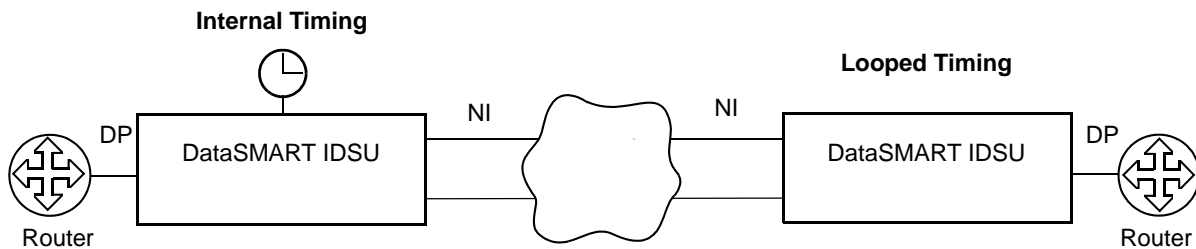
CLK:src

The *src* value specifies the source clock as:

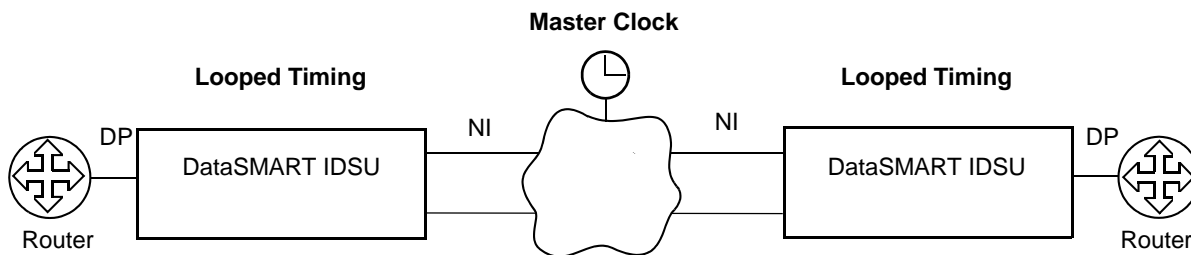
- L** Looped Timing (from the network receive signal)
- I** Internal Timing (using the IDSU internal oscillator)

The following illustrates some common timing applications for a T3 or E3 circuit.

Point-to-Point application: Span not timed by carrier



Timing setup: Span timed by carrier



Zeroing all counters

If you change the configuration parameters for the DataSMART T3/E3 IDSU, you may want to clear the performance database. You do this by zeroing all counters with the **ZALL** command. You must have super-user or configuration privileges.

The **ZALL** command clears the data from the following:

- User NI Short and Long Performance reports
- Far-End PRM Short and Long Performance reports
- User NI Statistical Performance report
- Alarm History report

The command also resets the alarm output relay. It does not clear SNMP counters.

Obtaining product version information

To obtain the model and serial numbers of your DataSMART T3/E3 IDSU to have available to give to your Customer Support representative, use the **WYV** command. You need super-user, configuration, or maintenance privileges.

The DataSMART T3/E3 IDSU displays the version information on the screen, similar to the following.

```
KENTROX      01-72555001, SERIAL 00614654,  
STAT 45E, ROM VER 3.22, S/W VER 1.31  
DSU Board Version 4
```

Resetting to default values

You can reset the DataSMART T3/E3 IDSU to its default power-up state at any time by using the **RSD** command. You must have super-user or configuration privileges.

When you enter the **RSD** command, the DataSMART T3/E3 IDSU:

- Logs out all users
- Restarts its control program and executes a self test
- Resets all configuration parameters to their default state
- Zeroes counters in the performance reports and clears the Alarm History report

Once self-test has been completed, you can log into the unit.



CAUTION!

A reset to defaults causes a service disruption until the DataSMART T3/E3 IDSU is reconfigured for service.

Resetting via the front panel

You can also reset the unit via the front panel. Set the front-panel thumbwheel switch to 3, then depress the ACTV and ACO buttons for 2.5 seconds.



NOTE

*You can reset the unit from the front panel at any time. The **DFP** command disables the front-panel switch from setting or resetting loopbacks, but not from resetting the unit defaults.*



CAUTION!

To avoid someone inadvertently resetting the unit, do not leave the thumbwheel switch set to 3. It is best to leave the switch set to 0.

Configuring the control port

The first step to configuring the control port for operation is to set the IDSU communication switches for baud rate, parity, stop and data bits. These switches are located on the IDSU circuit board and are described in your installation guide. The switches must be set to match the settings of your control device, or your control device must be set to match the switches. The factory-configured defaults for the switches are 9600 baud, 8 data-bits-per-second, 1 stop-bit-per-second, and no parity.

The user interface software allows you to view the control port communication settings and to turn “command echo” on or off.

The commands are listed in the Control Port Configuration menu. To display this menu, enter **CC** at the prompt.

```
CONTROL PORT CONFIGURATION MENU

EE / DE          - Enable/Disable Character Echo
CCV              - View Control Port Configuration
```

Viewing the current configuration

You can look at the current control port settings by executing the **CCV** command. This command displays the View Control Port Configuration screen, as shown below.

```
View Control Port Configuration

Echo      CP Setup
-----  -----
Enabled   96,N,8,1
```

Field	Description
Echo	This field tells you if character echo is enabled or disabled.
CP Setup	This field tells you the settings of the control port: baud rate in hundreds, parity, data-bits-per-character, and stop-bits-per-character.

Enabling/disabling character echo

When character echo is enabled, all printable characters sent to the control port are echoed back to the control device (e.g., characters are echoed on the screen of the control device). If character echo is disabled, characters are not echoed back to the control device.

The default for character echo is “enabled”.

To enable or disable character echo, use the **EE** and **DE** commands, respectively. You must have super-user or configuration privileges.

```
EE          Enable character echo
DE          Disable character echo
```

Configuring alarms

As part of the overall system setup, you can specify the format and types of alarm messages output by the DataSMART T3/E3 IDSU. You can:

- Enable or disable the alarm relay connector
- Enable or disable the generation of alarm messages
- Specify the alarm message format as ASCII or numeric (for compatibility with the Kentrox T-SMART Supervisor or MultiSMART Manager)
- Enable alarm dial-out and specify the number sent to the modem
- Specify whether or not alarms should be generated on incoming yellow and/or AIS conditions
- Specify the errored second and unavailable second thresholds for EER alarms
- Specify the duration of the DataSMART T3/E3 IDSU alarm deactivation period

This section describes how to set up the configuration parameters for alarms. If you enable alarms, you may also need to specify which control port you are using (the DCE or the DTE port), so that alarms are output correctly. By default, the alarms are output to DCE.

If you are using an SNMP network management tool, you will also need to make sure your SLIP interface is properly configured so that traps are sent to the right destination (see [Chapter 7, “Using Telnet and SNMP”](#)).

The commands for configuring alarms are listed in the Alarm Configuration menu. To display this menu, enter **AC** at the prompt.

```

ALARM CONFIGURATION MENU

EAR / DAR      - Enable/Disable Alarm Relay
EAM / DAM      - Enable/Disable Alarm Messages
EUM / EMM      - User/Manager Alarm Message Format
DIR / DDD      - Direct/Dialout Alarm Message Output
EMS:<str>      - Enter Modem String, str = AT command(s)

EYL / DYL      - Enable/Disable YELLOW Activating the Alarm
EAI / DAI      - Enable/Disable AIS Activating the Alarm
EST:<n>        - Errored Second Threshold, n = 0 .. 900
UST:<n>        - Unavailable Second Threshold, n = 0.. 900

ACV            - View Alarm Configuration

AC>

```

Viewing the current configuration

Before changing the alarm configuration parameters, you may want to look at the current settings. You can do this by executing the **ACV** command. This command displays the View Alarm Configuration screen, as shown below.

```

View Alarm Configuration

Relay      Message      Output      Modem String
-----
Disabled   Disabled   Direct
-----

Alarms Activated  EST  UST
LOS+OOF
-----
+YEL+AIS+EER      65  10

AC>

```

Field	Description
Relay	This field tells you if the alarm relay connector is enabled or disabled.
Message	This field tells you if alarm messages are enabled or disabled. If alarms are enabled, the field tells you the message format, either USER (ASCII) or numeric (suitable for use with the Kentrox T-SMART Supervisor or MultiSMART Manager).
Output	This field tells you whether alarms are output to the control port as soon as they occur (Direct), or if they are preceded by a dial-out number and held until an attached modem is ready (Dialout). This field applies to stand-alone units only because alarm dial-out is disabled in daisy-chained units.
Modem String	This field lists the string of AT commands and phone number sent to the modem when an alarm occurs. This applies only to stand-alone units set to a Dialout output mode.

Field	Description
Alarms Activated	This field tells you what types of conditions generate alarms. LOS and OOF always generate alarms. You can enable or disable alarms for incoming yellow (RAI) or AIS, or for EER conditions.
EST, UST	These fields tell you the alarm thresholds for errored second (ES) and unavailable second (UAS), respectively. The threshold count is accumulated in a sliding 15-minute time period. A zero (0) value means that EER alarms for ES or UAS have been disabled.

Enabling/disabling the alarm relay connector

The DataSMART T3/E3 IDSU provides an alarm relay connector on its back panel. You can use this alarm relay to trigger an external alarm whenever the IDSU detects an alarm condition.

The relay provides both normally-open and normally-closed contacts. If the alarm relay is enabled, you can use an “open-to-closed” or “closed-to-open” transition on the contacts to trigger the external alarm.

The default for alarm relay is disabled.

The state of alarm relay is stored in the permanent nonvolatile configuration database.

To enable or disable the alarm relay, use the **EAR** or **DAR** command. You need super-user or configuration privileges.

EAR	Enable alarm relay output
DAR	Disable alarm relay output

Enabling/disabling alarm messages

The DataSMART T3/E3 IDSU outputs an alarm message to your control device when it enters an alarm state. This message identifies the alarm type, the time and date of the alarm occurrence, and the device name and address of the IDSU sending the message.

You must disable this alarm message output if you are establishing a SLIP connection through the IDSU control port. With SLIP, alarms are output as SNMP traps.

The default for alarm message output is disabled.

NOTE

Disabling alarm messages does not disable SNMP traps. Nor does it disable the other alarm reporting mechanisms in the DataSMART T3/E3 IDSU, including the Alarm History report, the System Status report, and LED illumination.

To enable or disable alarm messages from the command line, use the **EAM** and **DAM** commands. You need super-user or configuration privileges.

EAM	Enable alarm messages
DAM	Disable alarm messages

Formatting the alarm messages (ASCII or numeric)

The DataSMART T3/E3 IDSU outputs alarm messages in one of two formats:

- ASCII, suitable for terminals and printers
- Numeric, suitable for use with the Kentrox T-SMART Supervisor and MultiSMART Manager

Specify the format appropriate for your application.

The default alarm format is ASCII.

To specify the message format, use the **EUM** and **ESM** commands. You must have super-user or configuration privileges.

EUM Output alarm messages in the ASCII format

ESM Output alarm messages in numeric format for T-SMART Supervisor and MultiSMART Manager

Enabling alarm dial-out

When alarm output is enabled (by the **EAM** command), the DataSMART T3/E3 IDSU outputs alarm messages to the control device as soon as they occur. In stand-alone applications, where the control device is connected via an ASCII interface (i.e., not SLIP), you can preface alarm messages with a dial-out string to an AT-compatible modem. The IDSU then holds the actual alarm message until the modem responds to the dial-out string.

There are two restrictions to this type of application:

- The alarm messages must be output to the DTE control port (use the **DTE** command).
- The modem connected to the DTE control port must be AT-compatible and set up as described in [Table 2](#).

You enable alarm dial-out by using the **DDD** command as described below. Before using this command, however, you must program the IDSU dial-out string using the **EMS** command as described on [page 36](#). If you have not programmed the dial-out string, the IDSU returns an error message when you enter the **DDD** command.

The default for alarm dial-out is disabled.

The status of alarm dial-out is stored in the permanent nonvolatile configuration database.

To enable or disable alarm dial-out you must have super-user or configuration privileges.

DIR Output alarm messages directly (i.e., disable alarm dial-out)

DDD Preface alarm messages with a dial-out string (i.e., enable alarm dial-out)

Table 2—Required AT settings for dial-out modem

AT setting	Description
ATS0=1	Auto answer on first ring
AT&C1	Assert DCD when the phone connection is made

Table 2—Required AT settings for dial-out modem (continued)

AT setting	Description
AT&D1	Transition modem from in-line to command mode when DTR transitions from on to off
ATQ1	Quiet on
ATE0	Echo off

Programming the dial-out string

The dial-out string can include up to 30 characters, comprising up to ten AT commands. One of the commands must be the ATD command specifying the remote phone number. The other commands are user-selectable.

An example command string:

EMS:ATLO;ATD5036431681

This command turns the volume of the modem to low, then dials the phone number 503-643-1681.

Note that the AT commands must be separated by semicolons (;). Commas insert a delay of two seconds. For example, the command:

EMS:ATLO;ATD503,6431681

This command turns the volume of the modem to low, then dials the phone number with a two-second delay after the area code.

Enabling/disabling alarms on incoming yellow (or RAI)

The DataSMART T3/E3 IDSU generates an alarm message if it detects an incoming yellow condition (a.k.a., Remote Alarm Indication (RAI) signal) at the network interface, and thus notifies you of a far-end problem. If you do not want this notification, you can deactivate this alarm message.



NOTE

These commands do not affect the IDSU's output of a yellow condition. The IDSU outputs yellow to the network when the IDSU enters an LOS or OOF state.

The default is to generate an alarm message on incoming yellow (enabled).

To enable or disable activation of an alarm on incoming yellow, use the **EYL** and **DYL** commands. You must have super-user or configuration privileges.

EYL Enable alarm activation on incoming yellow

DYL Disable alarm activation on incoming yellow

Enabling/disabling alarms on AIS

The DataSMART IDSU generates an alarm message if it detects AIS at the network interface. AIS tells you that some device upstream of the network is in an LOS or OOF alarm. If you do not want this notification, you can deactivate this alarm message.



NOTE

The IDSU does not generate AIS because it is an endpoint in the circuit.

The default is to generate an alarm message on incoming AIS (enabled).

To enable or disable activation of an alarm on incoming AIS, use the **EAI** and **DAI** commands. You must have super-user or configuration privileges.

EAI Enable alarm activation on incoming AIS

DAI Disable alarm activation on incoming AIS

Setting the threshold for errored seconds (ES)

You can specify that the DataSMART T3/E3 IDSU generate an EER alarm on excessive errored seconds (ESs). This allows you to monitor the line for errors and detect problems that are not described solely by signal loss (LOS) or out-of-frame (OOF) alarms.

An errored second is any second that is not an unavailable second and that contains one or more errored events: i.e., a transition to LOS, a transition to OOF, or a code violation.

You set up an EER alarm on excessive ESs by using the **EST** command to specify the error threshold. The threshold count is calculated within a sliding 15-minute time window. You can specify a threshold count of 0 to 900, inclusive. A value of 0 disables EER alarm activation on errored seconds; a value of 900 means that an alarm will be generated if an ES occurs every second of a 15-minute time window (60 x 15).

The default threshold is 65 errored seconds.

To set the ES threshold, use the **EST** command. You need super-user or configuration privileges. The command syntax is:

EST:*n*

n Enter the number of ESs that must occur within the time window in order to activate an EER alarm. The allowed values are 0 to 900, inclusive. 0 disables EER alarm activation on an ES condition.

Setting the threshold for unavailable seconds (UAS)

If your line is experiencing chronically high error rates, you may elect to disable the errored second (ES) threshold and just use the unavailable second (UAS) threshold for generating EER alarms. This decreases the alarm sensitivity significantly, since a UAS occurs at the onset of ten consecutive severely errored seconds (SESSs), which are defined as errored seconds having 44 or more error events.

You use the **UST** command to specify the threshold used for generating an EER alarm on UASs. The threshold count is calculated within a sliding 15-minute time window. You can specify a threshold value of from 0 to 900, inclusive. A value of 0 disables EER alarm activation on unavailable seconds; a value of 900 means that an EER alarm will be generated if an unavailable second occurs every second of a 15-minute time window.

The default threshold is 10 unavailable seconds.

To set the UAS threshold, use the **UST** command. You need super-user or configuration privileges. The syntax for the command is:

UST:*n*

n Enter the number of UASs that must occur within the time window in order to activate an EER alarm. The allowed values are 0 to 900, inclusive. 0 disables alarm activation on a UAS condition.

4

Configuring interfaces

This chapter covers the following topics:

- Configuring the network interface
- Configuring the data port interface

Configuring the network interface

Configure the DataSMART T3/E3 IDSU network interface to be compatible with the T3 or E3 signal received from your service provider. It is particularly important to match the network interface framing to that of the received signal. Other parameters are less critical, and the defaults supplied by the DataSMART T3/E3 IDSU work for most applications.

The commands for configuring the network interface parameters are listed in the Network Interface (NI) Configuration menu. To display this menu, enter **NC** at the prompt.

```
NI CONFIGURATION MENU

NM13 / NCBT / NE3 - T3 M13, T3 C-Bit Parity, or E3 NI Framing Format
NLO  / NHI      - Low/High NI Transmit Output Level
LBO:<IN or OUT> - Sets the transmit Line Build Out to be IN or OUT

NCV              - View NI Configuration

NC>
```

Viewing the current network interface configuration

You can view the current network interface configuration by displaying the View NI Configuration. Enter **NCV** at the prompt.

```
View NI Configuration

Framing      Transmit      Transmit
Format       Output Level  LBO
-----
T3 M13      Low           Out

NC>
```

Field	Description
Framing Format	This field displays the current network framing: T3 M13, T3 C-bit parity, or E3 framing format.
Transmit Output Level	This field tells you the current transmit level of the network output signal. A Low setting is used for cabling distances of less than 450 feet; a High setting (which amplifies the pulse) is used for cabling distances of 450 feet or greater.
Transmit LBO (Line Build Out)	This field tells you the current attenuation setting of the network output signal. For T3, an In (enabled) setting is used for cabling distances of less than 225 feet; an Out (disabled) setting is used for cabling distances of 225 feet or greater. Line attenuation is always disabled for E3 framing.

Specifying NI framing format

Set the framing format to match the format of the receive (input) signal at the network interface. Two T3 framing formats are supported:

NCBT Set the framing format to T3 C-Bit Parity

NM13 Set the framing format to T3 M13 framing

One E3 framing format is supported:

NE3 Set the framing format to E3 CCITT G.751 standard

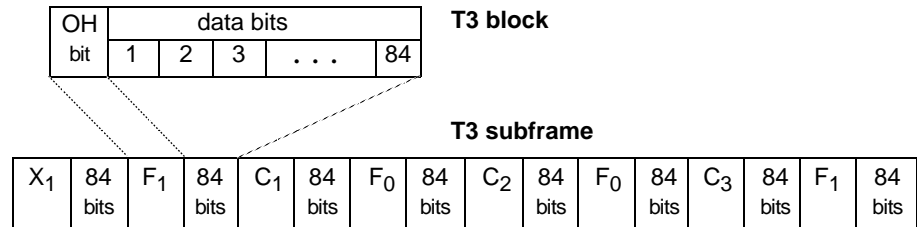
The default framing format is T3 M13.

The status of the framing format is stored in the permanent nonvolatile configuration database.

You must have super-user or configuration privileges to change the framing format.

T3 framing formats

The T3 block comprises one overhead bit (OH) and 84 data bits. The T3 subframe comprises eight T3 blocks. Seven T3 subframes compose one T3 frame.



C-Bit Parity frame The following illustration shows the overhead bits contained in a C-Bit Parity frame.

F and M bits are used for framing and alignment

X bits transmit failure conditions from the far-end to the near-end

P bits contain parity information

C bits AIC = Application Identification Channel

Nr = Reserved Network Requirement bit

FEAC = Far-end Alarm bit

DL = Data Link bits

CP = C-Bit Parity bits

FEBE = Far-end Block Error bits

X ₁		F ₁		AIC		F ₀		N _r		F ₀		FEAC		F ₁	
X ₂		F ₁		not used		F ₀		not used		F ₀		not used		F ₁	
P ₁		F ₁		CP		F ₀		CP		F ₀		CP		F ₁	
P ₂		F ₁		FEBE		F ₀		FEBE		F ₀		FEBE		F ₁	
M ₀		F ₁		DL		F ₀		DL		F ₀		DL		F ₁	
M ₁		F ₁		not used		F ₀		not used		F ₀		not used		F ₁	
M ₀		F ₁		not used		F ₀		not used		F ₀		not used		F ₁	

M frame The following illustration shows the overhead bits contained in a T3 M frame.

- F and M bits are used for framing and alignment
- X bits transmit in-service messages and yellow alarm
- P bits contain parity information
- C bits contain T3 bit stuffing indicators

X ₁		F ₁		C ₁		F ₀		C ₁₂		F ₀		C ₁₃		F ₁	
X ₂		F ₁		C ₂₁		F ₀		C ₂₂		F ₀		C ₂₃		F ₁	
P ₁		F ₁		C ₃₁		F ₀		C ₃₂		F ₀		C ₃₃		F ₁	
P ₂		F ₁		C ₄₁		F ₀		C ₄₂		F ₀		C ₄₃		F ₁	
M ₀		F ₁		C ₅₁		F ₀		C ₅₂		F ₀		C ₅₃		F ₁	
M ₁		F ₁		C ₆₁		F ₀		C ₆₂		F ₀		C ₆₃		F ₁	
M ₀		F ₁		C ₇₁		F ₀		C ₇₂		F ₀		C ₇₃		F ₁	

E3 framing format

The following illustration shows the E3 framing block.

- FAS contains the 10-bit frame alignment signal
- A is the alarm bit
- N is the national bit
- 1100 is the stuff sequence

FAS	A	N	1100	190 octets payload
-----	---	---	------	-----------------------

Setting the output level of the transmit signal

If the cabling distance between your IDSU and the service provider's network interface unit (NIU) is 450 feet or longer, you need to amplify the output pulse from the IDSU. The normal output pulse is appropriate for applications that use cabling of less than 450 feet.

The default setting is "no amplification", which is appropriate for cabling of less than 450 feet.

Use the following commands to specify the transmit output level. You must have super-user or configuration privileges.

The status of amplification is saved in the permanent nonvolatile configuration database.

NLO Do not amplify the signal pulse (for cabling less than 450 feet)

NHI Amplify the signal pulse (for cabling of 450 feet or greater)

Specifying transmit line build-out attenuation

NOTE

This field applies to T3 framing only; line build-out is disabled for E3.

If the cabling distance between your IDSU and the service provider's network interface unit (NIU) is less than 225 feet, you usually need to reduce or attenuate the network transmit signal. You should verify this with your service provider.

The default setting is "no attenuation", which is appropriate for cabling distances of 225 feet or greater.

Use the following to specify attenuation. You must have super-user or configuration privileges.

LBO:IN Attenuate the network output signal (for cabling less than 225 feet)

LBO:OUT Do not attenuate the network output signal (for cabling of 225 feet or greater)

Configuring the data port

The DataSMART T3/E3 IDSU has two physical data ports located on its rear panel: a HSSI port and a user-programmable V.35/EIA-530 data port. You can use either port, but not both at the same time.

You must configure the data port you are using to match the configuration of the data terminal equipment (DTE) to which it is attached.

The commands for configuring the data ports are listed in the System Configuration menu. To view this menu, enter **SC** at the prompt.

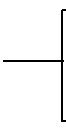
```

                                SYSTEM CONFIGURATION MENU

SD:<mmm>,<dd>,<yy>    - Set Date
ST:<hh>:<mm>          - Set Time
SN:<id>              - Set Name
SA:<xx>:<yy>:<zzz>    - Set the Unit's Address to slot:shelf:group
EFP / DFP           - Enable/Disable Front Panel Operation
DCE / DTE           - DCE/DTE is the Alarm Output Port
CLK:<src>            - Clock Source, src = I (Internal), L (Looped)
DSUCLK:<xx.x>,<yy.y> - Sets DSU data port clock (direction is NI)
                    xx.x = transmit, yy.y = receive
HSSI / V35 / EIA530 - Select data port as HSSI, V.35 or EIA-530
ESCRAM/DSCRAM       - Enable/Disable Scrambling on the DSU Data Port
ZALL                 - Zero All Counters used in User Reports
WYV                  - What's Your Version
RSD                  - Reset Unit to Dip Switch Defaults
SCV                  - View System Configuration

SC>
```

These commands program the data port.



Viewing the current data port configuration

Before changing any data port parameters, you may want to look at the current settings. To do this, enter **SCV** at the command-line prompt. This produces a display similar to the one shown below.

```

View System Configuration

Date           Time      Name           Address
-----
JAN 14, 1990  21:14  PORTLAND,OR    00:00:000

Timing         Front Panel Port  Data Port  Transmit Clock  Receive Clock
-----
Looped         Enabled    DCE  HSSI         45.0 MHz  45.0 MHz

Scrambling
-----
Disabled

SC>

```

These fields report the status of the data port configuration.

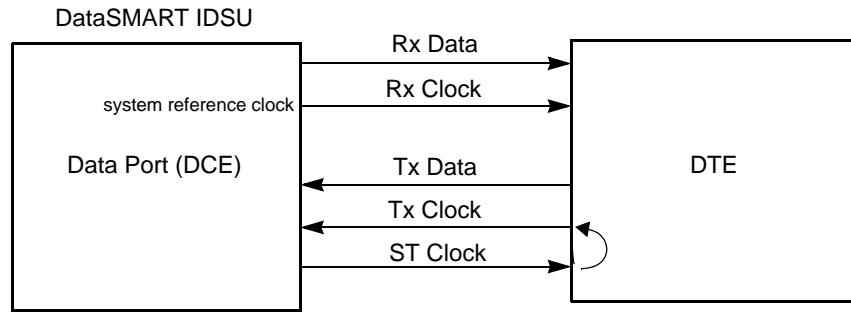
Field	Description
Data Port	These fields tell which physical interface is being used: HSSI, V.35 or EIA-530.
Transmit Clock	This field identifies the clock rate used for clocking data input at the data port (transmit data from the DTE).
Receive Clock	This field identifies the clock rate used for clocking data output at the data port (receive data from the network).
Scrambling	This field tells you whether or not data scrambling is enabled at the port. For most applications, scrambling should be left disabled.

Setting the transmit and receive clock rate

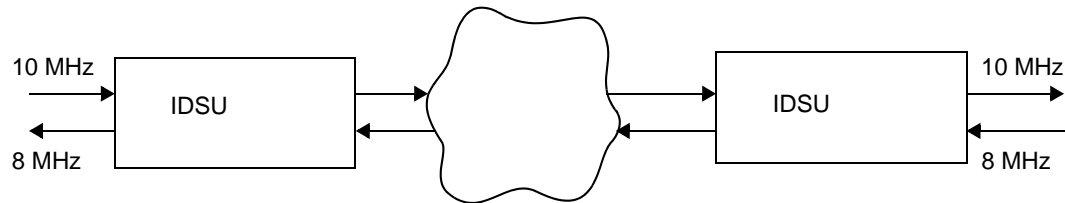
Transmit (input) and receive (output) timing at the data port is sourced from the IDSU system reference clock. This clock is either the internal IDSU clock or a clock derived from the network receive signal (as specified by the **CLK** command, see [page 28](#)).

The IDSU outputs the receive data and receive clock to the DTE. It also outputs a clock signal (ST) to the DTE, which the DTE loops and returns as its transmit clock. The DTE must be able to loop the IDSU clock signal; the IDSU data port cannot slave from an external clock supplied by the DTE.

Figure 2—Data port clock



You can specify the clock rates used for transmit and receive timing at the data port. These clock rates can be different from each other, depending on how you want to shape traffic to and from your DTE. When shaping traffic, be aware that the transmit and receive timing at the near- and far-ends should be synchronized. For example,



The clock rates are specified in increments of 0.5 MHz. The maximum rates allowed depend on the network type and data port type. If you are using a HSSI port, the highest data rates (45 MHz for T3 and 34 MHz for E3) are only available if both the transmit and receive rates are set to the maximum.

Table 3—Multi-rate timing

Network type	Data port type	Allowed range
T3 or E3	V.35 or EIA-530	1 to 8.0 MHz
T3	HSSI	1 to 35 MHz; or 45 MHz if both transmit and receive are set to 45 MHz
E3	HSSI	1 to 24.5 MHz; or 34 MHz if both transmit and receive are set to 34 MHz

The defaults for the clock rates are 4 MHz for V.35 or EIA-530, 45 MHz for T3 HSSI, and 34 MHz for E3 HSSI.

Use the following command to set the receive and transmit clock rates for the data port. You must have super-user or configuration privileges.

The clock rates are stored in the permanent nonvolatile configuration database.

DSUCLK:*xx.x,yy.y*

xx.x Set the transmit clock to a 0.5 MHz resolution of the allowed range, see [Table 3 on page 47](#).

yy.y Set the receive clock rate to a 0.5 MHz resolution of the allowed range, see [Table 3 on page 47](#).

Specifying the physical interface

You need to specify the physical interface for the attached data terminal equipment (DTE): HSSI, V.35, or EIA-530.

The default port setting is HSSI. To change the setting, you need super-user or configuration privileges.

The port setting is stored in the permanent nonvolatile configuration database.

HSSI The DTE is connected to the 50-pin HSSI interface.

V35 The DTE is connected to the 25-pin D connector and is V.35 compatible.

EIA530 The DTE is connected to the 25-pin D connector and is EIA-530 (or EIA-449, RS449) compatible.

Enabling/disabling payload scrambling

Payload scrambling reduces the pattern sensitivity of fiber-optic multiplexing equipment (often used by the carrier of T3 or E3 lines). If the IDSU is receiving AIS at the network when you know the transmit signal from the IDSU is fine, you should try scrambling the payload of the signal. The unscrambled bit pattern might be triggering a false alarm in the carrier multiplexer.

The default is payload scrambling disabled.

The status of payload scrambling is stored in the nonvolatile configuration database.

To change the status of payload scrambling, use the following commands. You must have super-user or configuration privileges.

ESCRAM Enable scrambling

DSCRAM Disable scrambling

5

Performance monitoring

This chapter describes how to monitor the performance of the incoming T3 or E3 circuit by using the various reporting facilities available from the DataSMART T3/E3 IDSU.

Though this chapter describes different reports, learning to understand them is simplified by the fact that many are similar in format. For instance, all these reports are similar:

- User NI report
- Far-end report
- Subrate Data report

Because of the similarities of these reports, the easiest way to learn about them is to learn the most commonly-used report first, which is the User NI report. Descriptions of all other reports of the same type refer back to the description of the User NI report.

This chapter also describes two other reports:

- User NI Statistical Performance report
- Alarm History report

The chapter is organized as follows:

- The first section shows how to access the various reports.
- The next five sections show how to interpret the reports.

Though the reports described here contain some information about alarm status, the System Status report, described in [Chapter 6](#), has more complete information. See “[Examining system status](#)” on page 64.

Accessing reports

The Reports menu lists commands for accessing reports. To view this menu, log into the plug-in and enter **R**.

```
PERFORMANCE REPORT MENU

UNSR / UNLR - User NI Short/Long Performance Report
FESR / FELR - Far End PRM Data Short/Long Performance Report
SDLR       - Subrate Data Long Performance Report

NSR        - User NI Statistical Report
AHR        - Alarm History Report

PL:<n>     - Page Length, n = 20 .. 70, (P - Page Break) (V - View)

R >
```

To display any report, simply enter the appropriate command from the command line. You do not need any special privilege level.

Some reports have a long or short version. The long version differs from the short version only in that it includes a break-down of the performance information for the previous 24 hours, shown in 15-minute intervals.

For example, use these commands to display the User NI reports.

UNSR	Display the short version of the User NI report
UNLR	Display the long version of the User NI report

TIP

For information on these and other reports, see the sections on interpreting performance reports starting on [page 52](#).

Controlling page length

Using the **PL** (page length) command, you can set the page length of a report from 20 to 70 lines. If the report exceeds the page length on the screen, the IDSU displays the prompt

“Continue? (Y/N for yes or no)”

at the end of a page. You can then display the next page of the report by typing **Y**, or you can end the report display by typing **N**.

If you are printing the report to a printer, you can replace the screen “Continue?” prompt with a printer page break consisting of a Ctrl-L form-feed character. This tells the printer when to break the page. You specify a printer page break by including the **P** parameter with the page length command (see below).

A page length of 0 disables both page breaks and prompting.

By default, no page length is specified and page breaks and prompting are disabled. If you enter a page length, the command defaults to a “Continue?” screen prompt.

The **PL** command syntax is:

PL:*n*[**P** | **V**]

- n* Specify the page length as **0**, **20** ... **70**. 0 disables page breaks and prompting.
- P** Specify **P** for “page break”. This tells a printer to insert a line feed at the end of a page.
- V** View the current page length settings. A display similar to the one shown below appears.

```
Page Length      : 0
Page Break       : No
Continue Prompt  : No
```

For example, to fit a report on a 22-line monitor, enter:

PL:22

Clearing the performance database

At any time, you can clear the performance data and reset counters by executing the **ZALL** command (see [“Zeroing all counters” on page 29](#)). The **ZALL** command clears the data from all reports except the Carrier NI report and the Alarm History report.

Performance data is also cleared whenever you reset the date or time on the DataSMART T3/E3 IDSU using the **ST** or **SD** commands (see [“Setting date and time” on page 25](#)).

You lose performance data and alarm history data if you cycle power to the DataSMART T3/E3 IDSU.

If you use the **RSD** command to reset the DataSMART T3/E3 IDSU to its defaults (see [“Resetting to default values” on page 30](#)), you lose the current alarm history data, performance data, and configuration settings. Use the **RSD** command with caution.

Interpreting the User NI report

The DataSMART T3/E3 IDSU monitors the received signal at the network interface for a variety of error conditions. The DataSMART T3/E3 IDSU logs the errors and then uses the log to determine the quality of the 1-second interval during which the errors occurred.

For each time interval, the DataSMART T3/E3 IDSU tallies the counts and displays the information in the report. The report also shows the error conditions and whether or not an alarm was present.

The following figure shows an example of the User NI Short Performance Report (UNSR).

```

                                KENTROX DataSMART T3/E3 IDSU
                                USER NI SHORT PERFORMANCE REPORT
ADDRESS: 00:00:000                NAME: PORTLAND,OR

DATE: JAN 14, 1990                TIME OF DAY: 00:27

Status Codes:
L = LOS, O = OOF, E = EER, A = AIS, Y = YELLOW,
@ = ALARM ACTIVE,
T = TEST ACTIVE

                                CODE          ERRORED   BURSTY    SEV ERR   UNAVAIL
                                VIOLATIONS  SECONDS   SECONDS   SECONDS   SECONDS   STATUS
                                -----
Cur Sec                        0          0         0         0         1   L   @
Pre Sec                         0          0         0         0         1   L   @
Cur 15-min                     0          0         0         0        627  L   @
Pre 15-min                      0          0         0         0        900  L   @
Cur 24-hr                      0          0         0         0       2898  L   @

R >
```

Time intervals in the short report

The short report shows the performance data for the current second, the previous second, the current 15-minute period, the previous 15-minute period, and the current day.

Each day is broken into ninety-six 15-minute intervals. Interval one starts at 00:00 (midnight), interval two at 00:15, interval three at 00:30, and so on.

“Cur 15-min” refers to the performance data tabulated so far for the 15-minute interval. For instance, in the previous figure, the third row shows the performance for the 15-minute interval starting at 00:15 (notice that the time of day is 00:27).

A zero (0) indicates that the plug-in was collecting data and the count for that field was zero.

Time intervals in the long report

The long report (use the **UNLR** command) shows the same information as the short report and also includes performance data for each complete 15-minute interval in the current 24 hours (that is, the previous ninety-six 15-minute intervals). If not all of the 15-minute intervals are listed, it means the DataSMART T3/E3 IDSU has not been on for 24 hours.

The following figure shows the additional information provided by the long version of the User NI report (**UNLR**).

```
.
:
:
Time Accumulated
02:30          0          0          0          0          0
02:15          0          0          0          0          0
02:00          0          0          0          0          0
01:45          0          0          0          0          0
01:30          0          0          0          0          0
01:15          0          0          0          0          0      E   @
01:00          21         20          0          0          2      E   @
00:45         523        523          0          7          9   LOEA @
00:30          76         68          0          0          2      E   @
00:15          0          0          0          0          0      E   @
.
:
:
```

Performance measurements

For each time interval there are six types of performance measurements. These measurements are described below.

Field header	Definition
CODE VIOLATIONS	For T3 M13 framing, code violations consist of P-bit errors, F-bit errors, M-bit errors, and/or B3ZS encoding violations. For T3 C-bit parity framing, code violations consist of CP-bit errors, F-bit errors, M-bit errors, and/or B3ZS encoding errors. For E3 framing, code violations represents the number of LCVs that have been detected, where an LCV is defined as two consecutive bipolar violations (BPVs) of the same polarity.
ES	An errored second (ES) is any second that contains at least one code violation.
BES	A bursty errored second (BES) is any second with more than 1 but less than 44 code violations.
SES	A severely errored second (SES) is any second with 44 or more code violations.
UAS	An unavailable second (UAS) is declared at the onset of 10 consecutive SESs; it is cleared at the onset of 10 consecutive non-SESs.
STATUS	This column shows the type of errored conditions that occurred during the time interval: L An LOS condition (but not necessarily an alarm) has occurred. O An OOF condition (but not necessarily an alarm) has occurred. E An Excessive Error Rate (EER) alarm has occurred. A An AIS condition (but not necessarily an alarm) has occurred. Y A yellow (AFA) alarm has been detected. @ There is an alarm state active on the DataSMART T3/E3 IDSU. T There is a (loopback) test active on the DataSMART T3/E3 IDSU.

Interpreting the Far-end report (available only for T3 C-Bit framing)

Far-end reports are based on PRMs, and PRMs are only defined for the T1 C-Bit Parity mode of framing. Therefore, far-end reports are only available when the network interface is set to T3 C-Bit framing.

The **FESR** and **FELR** commands display the recent performance history of the received signal at the far-end network interface. The reports generated by the commands are similar to the User NI report. However, the data for the Far-end report is received from the remote device through Performance Report Messages (PRMs).

Because the Far-end reports are based on PRMs, PRM generation must be enabled in the far-end device.

The figure below shows an example of a short version of the Far-end report. Notice that it is the same as a User NI report except for the status codes described in the header and listed in the status column.

```

                                KENTROX DataSMART T3/E3 IDSU
                                FARE END SHORT PERFORMANCE REPORT
ADDRESS: 00:00:000                NAME: PORTLAND,OR

DATE: JAN 14, 1990                TIME OF DAY: 00:27

Status Codes:
  T = TEST ACTIVE
  I = INCOMPLETE
  Y = RECEIVED YELLOW
  @ = FAR-END ALARM

                                CODE      ERRORED  BURSTY   SEV ERR  UNAVAIL
                                VIOLATIONS SECONDS  SECONDS  SECONDS  SECONDS  STATUS
                                -----  -
Cur Sec                        0         0        0         0         1  Y   @
Pre Sec                         0         0        0         0         1  Y   @
Cur 15-min                     0         0        0         0        627   I
Pre 15-min                      0         0        0         0         900   I
Cur 24-hr                      0         0        0         0        2898  I

R >
```

Interpreting the Subrate Data Performance report

The Subrate Data Performance report is available when IDUS data port clocking is set to rates lower than the maximum HSSI clock rates of 45 MHz for T3, or 34 MHz for E3. When data port clocking is set lower than the maximum rates, HDLC framing is used to “encapsulate” subrate data within the standard T3 or E3 frames. The Subrate Data Performance report gives you a breakdown of any encountered HDLC framing errors.

The **SDLR** command displays the recent HDLC performance history at the network interface. The report generated by the command is similar to the User NI Long report in terms of the time intervals counted. The performance data accumulated for those intervals is specific to HDLC framing.

The figure below shows an example of the Subrate Data Performance report. The table below the figure describes the column headers and performance data.

```

KENTROX DataSMART T3/E3 IDUS
SUBRATE DATA PERFORMANCE REPORT
ADDRESS: 00:00:000          NAME: PORTLAND,OR

DATE: DEC 11, 1996        TIME OF DAY: 00:47

Status Code:
  To = TRANSMIT FIFO OVERFLOW,   Tu = TRANSMIT FIFO UNDERFLOW
  Ro = RECEIVE FIFO OVERFLOW,    Ru = RECEIVE FIFO UNDERFLOW

RECEIVE ERRORS
-----
HEADER  LENGTH  FCS      TOTAL VALID  TOTAL VALID  FIFO
ERRORS  ERRORS  ERRORS   RECEIVED     TRANSMITTED  STATUS
-----
Cur Sec      0    510      0            0            0  ToRu
Pre Sec      0   5100     0            0            0  ToRu
Cur 15-min   0  16320    0            0            0  ToRu
Cur 24-hr   0     0       0            0            0
R >

```

Field header	Definition
HEADER ERRORS	The number of packets with invalid headers received during the time interval.
LENGTH ERRORS	The number of packets with invalid lengths received during the time interval.
FCS ERRORS	The total number of packets that failed the FCS (CRC-16) check during the interval.
TOTAL VALID RECEIVED	The total number of all valid data packets received and passed on to the DTE equipment.
TOTAL VALID TRANSMITTED	The total number of all valid data packets transmitted to the network.
FIFO STATUS	This column shows the FIFO status for the given time interval, where: <ul style="list-style-type: none"> To indicates a Transmit FIFO overflow Tu indicates a Transmit FIFO underflow Ro indicates a Receive FIFO overflow Ru indicates a Receive FIFO underflow

Interpreting the Statistical reports

A Statistical report provides a 24-hour performance summary on the received signal at the network interface. It shows you the number of available and error-free seconds that occurred within the last 24 hours, and calculates the percentages of total seconds represented by the available and error-free seconds. The report also shows you the number of code violations that occurred within the last 15 minutes and the last 24 hours.

```

                                KENTROX DataSMART T3/E3 IDSU
                                USER NI STATISTICAL PERFORMANCE REPORT
ADDRESS: 00:00:000                NAME: PORTLAND,OR

DATE: JAN 15, 1990                TIME OF DAY: 00:47

STATISTIC                          DATA
-----                          -----
Available Seconds in Last 24 Hours          0
Percentage of Available Seconds in Last 24 Hours  0.0%
Error Free Seconds in Last 24 Hours          0
Percentage of Error Free Seconds in Last 24 Hours  0.0%
Code Violations in Current 15 Minutes        0
Code Violations in Last 24 Hours            0

R >
```

An error-free second is a second that is not an ES (errored second), a BES (bursty errored second), an SES (severely errored second), or a UAS (unavailable second).

Available seconds are seconds that are not UAS.

The percentages are computed from the counts stored in the performance database for the User NI report.

Interpreting the Alarm History report

The Alarm History report (use the **AHR** command) shows the last 24 alarm messages. The alarm messages in the report are the same messages sent to the control port device when the control port alarm messages are enabled and configured for ASCII format.

A message is added to the report every time an interface changes to a different alarm state. The “Alarm Cleared” message is not issued unless all alarms on that line are cleared. The report logs up to 24 messages, most recent first. Once the report reaches 24 messages, subsequent messages cause the oldest message to be dropped.

See [“Monitoring alarm messages” on page 63](#) for a full list of the types of alarms messages that can appear in this report and their meanings.

The alarm messages are always displayed in user format, regardless of the Alarm Message Format defined with the **EUM/ESM** command is the Alarm Configuration menu.

Alarm messages will always appear in the Alarm History report, even if alarm messages were disabled with the **DAM** command in the Alarm Configuration menu.

Information in the Alarm History report is not cleared when an **ST**, **SD**, or **ZALL** command is executed. Only power cycling the plug-in or executing the **RSD** (reset system to default values) command under the System Configuration menu will clear the Alarm History report.

An example of the Alarm History report is shown below.

```
SET ALM JAN.13,1996 10:52 NI EER PORTLAND,OR      addr = 00:00:000
CLR ALM JAN.13,1996 10:52 NI PORTLAND,OR         addr = 00:00:000
SET ALM JAN.13,1996 10:51 NI YEL PORTLAND,OR     addr = 00:00:000
CLR ALM JAN.13,1996 10:50 NI PORTLAND,OR         addr = 00:00:000
SET ALM JAN.13,1996 10:47 NI YEL PORTLAND,OR     addr = 00:00:000
CLR ALM JAN.13,1996 10:31 NI PORTLAND,OR         addr = 00:00:000
SET ALM JAN.13,1996 10:18 NI EER PORTLAND,OR     addr = 00:00:000
SET ALM JAN.13,1996 10:18 NI OOF PORTLAND,OR    addr = 00:00:000
SET ALM JAN.13,1996 10:18 NI EER PORTLAND,OR    addr = 00:00:000
SET ALM JAN.13,1996 10:18 NI OOF PORTLAND,OR    addr = 00:00:000
SET ALM JAN.13,1996 10:18 NI LOS PORTLAND,OR    addr = 00:00:000
SET ALM JAN.13,1996 10:17 NI EER PORTLAND,OR    addr = 00:00:000
SET ALM JAN.13,1996 10:16 NI YEL PORTLAND,OR    addr = 00:00:000
SET ALM JAN.13,1996 10:16 NI EER PORTLAND,OR    addr = 00:00:000
SET ALM JAN.13,1996 10:16 NI LOS PORTLAND,OR    addr = 00:00:000
SET ALM JAN.13,1996 10:16 NI EER PORTLAND,OR    addr = 00:00:000
SET ALM JAN.13,1996 10:16 NI OOF PORTLAND,OR    addr = 00:00:000
SET ALM JAN.13,1996 10:16 NI AIS PORTLAND,OR    addr = 00:00:000
SET ALM JAN.13,1996 10:16 NI OOF PORTLAND,OR    addr = 00:00:000
SET ALM JAN.13,1996 10:16 NI LOS PORTLAND,OR    addr = 00:00:000
```

6

Troubleshooting

This chapter describes how to troubleshoot the DataSMART T3/E3 IDSU. It contains the following information:

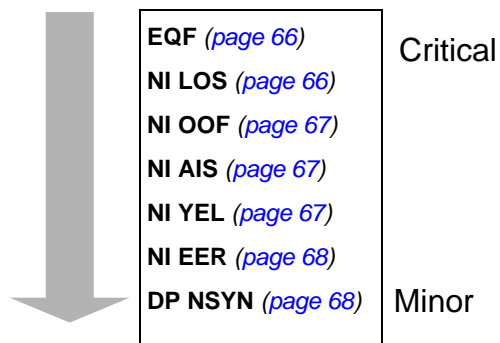
- How LEDs and alarm messages alert you when something is wrong
- How to find out the type of alarm which is occurring
- A list of all error conditions in the System Status report, and suggestions on how to resolve them
- A description of how to use the DataSMART T3/E3 IDSU diagnostic loopbacks

Following is a quick guide to the alarms generated by the DataSMART T3/E3 IDSU and to the pages in this chapter that provide appropriate troubleshooting procedures for the alarms. The alarms are listed in priority order, from critical to minor. Always deal with critical alarms first.

TIP

Always deal with critical alarms first.

Figure 3—Troubleshooting the DataSMART IDSU



Interpreting the front-panel LEDs

The front-panel LEDs provide an “on-site” way to alert you that the DataSMART T3/E3 IDSU is experiencing abnormal conditions. The following figures show the LEDs during normal and abnormal conditions.

Figure 4—LEDs when conditions are normal

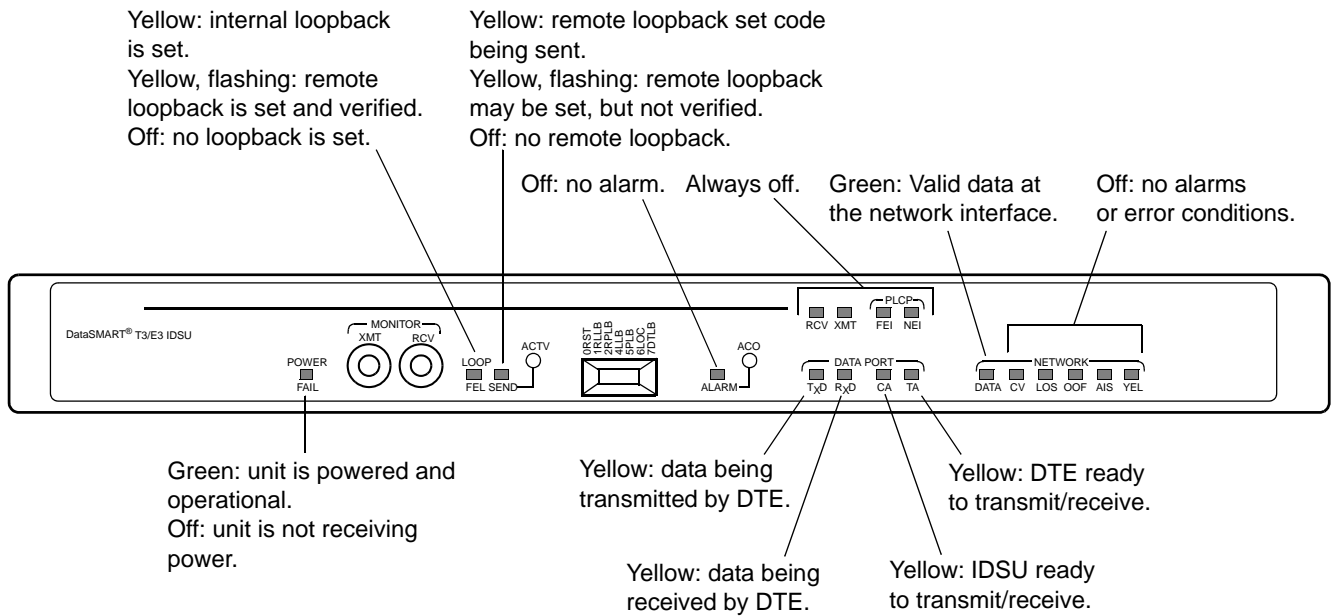


Figure 5—LEDs when conditions are abnormal

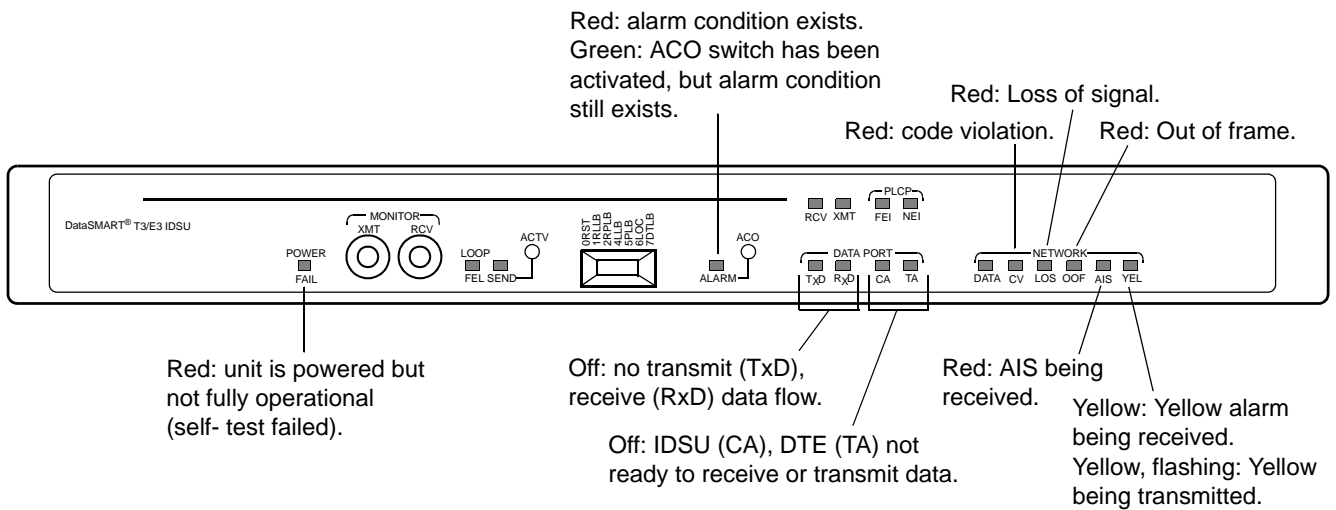


Table 4—LED indicators and their meanings

LED	Indicator	Condition
POWER/FAIL	Green	Power is on, self-test successful.
	Red	Power is on, self-test failed. The network LEDs show which tests failed. If AIS is lit, RAM read write test failed. If OOF is lit, NVRAM tests failed. If LOS is lit, EPROM has an invalid checksum.
	Off	No power is being received.
LOOP/FEL	Yellow	Internal loopback is set.
	Yellow, flashing	Remote loopback is set and verified.
SEND	Yellow	Remote loopback set code is being transmitted.
	Yellow, flashing	Remote loopback may be set but not verified.
ALARM	Red	Alarm exists at the network interface.
	Green	ACO switch has been activated, but alarm still exists at the network interface.
	Off	No alarm.
RCV XMT FEI NEI	Off	Not used; always off.
TxD	Yellow	Data is being transmitted by DTE, received by IDUSU. (Indicates SD activity for HSSI port, transmit data activity for V.35/EIA-530 port.)
	Off	No transmit data.
RxD	Yellow	Data is being received at DTE, transmitted by IDUSU. (Indicates RD activity for HSSI port, receive data activity for V.35 port.)
	Off	No receive data flow.
CA	Yellow	Indicates IDUSU is ready to send and receive data. (Indicates the state of the CA signal on the HSSI port, and state of CTS & DCD for V.35/EIA-530 port.)

Table 4—LED indicators and their meanings (continued)

LED	Indicator	Condition
	Off	IDSU not ready.
TA	Yellow	Indicates DTE is ready to send and receive data. (Indicates the state of the TA signal on the HSSI port, and DTR for V.35 port.)
	Off	DTE not ready.
DATA	Green	Valid framing is being received at the network interface.
CV	Red	Code violation detected at the network interface.
LOS	Red	Loss of signal detected at the network interface.
OOF	Red	Out-of-frame condition detected at the network interface.
AIS	Red	Alarm indication signal (AIS) is being received at the network interface.
YEL	Yellow	Yellow alarm is being received at the network interface.
	Yellow, flashing	Yellow alarm is being transmitted at the network interface.

Monitoring alarm messages

The DataSMART T3/E3 IDSU generates the alarm messages listed in [Table 5](#) and outputs them at the control port. If you receive an alarm message, you should use the Status (**SS**) command to get the details of the problem.

Only one alarm can be active at a time. If two alarm conditions exist, the IDSU issues an alarm message only for the higher priority alarm. When the higher priority alarm is cleared, the IDSU then issues the next lower priority alarm, if one is still present. The table shows the alarms in decreasing order of priority.

Table 5—Alarms generated by the DataSMART IDSU

Alarm	Description
EQF	DataSMART T3/E3 IDSU equipment failure at power-up.
NI LOS	Loss of T3 or E3 signal at the network interface.
NI OOF	Out-of-frame signal at the network interface. Some or all of the framing bits have been lost.
NI AIS	Incoming AIS (alarm indicator signal) at the network interface. Some device upstream of the network interface is in an LOS or OOF alarm state or in a test mode.
NI YEL	Incoming yellow alarm at the network interface. A device upstream of the network interface is in an OOF or LOS alarm state on the near side.
NI EER	Excessive error rate detected on the signal at the network interface.
DP NSYN	If the data port transmit and receive clocks are set to subrates (i.e., rates lower than the maximum HSSI clock rates), this alarm indicates that the data port is out of sync with the far-end. In other words, it is experiencing an overflow or underflow condition because the far-end is set to different clock rates. The alarm clears 5 seconds after the overflow or underflow condition clears.

Examining system status

If the DataSMART T3/E3 IDSU is in an alarm state or if you notice an abnormal condition, use the System Status report display to get more information. The status codes are explained in the table below.

The system status tells you the current condition of the DataSMART T3/E3 IDSU, including any alarms that may be active as well as current — and possibly intermittent— signal conditions at the network interface and the data port. The status display is dynamic and is updated as conditions change on the DataSMART T3/E3 IDSU.

Using the command line

To see the display, enter **S** at the prompt. A screen similar to the one shown below appears. The display is updated once per second if the status changes, with the new status line added at the bottom. You exit the display by pressing Ctrl-C.

The display contains three sections: System, NI (network interface), and DP (data port). The column headings under each section read vertically. If the condition described in the column heading is present, an asterisk appears under the column. A dash means the condition is not present.

```
OPERATIONAL STATUS (* Yes, - No, ^C to Exit)
      JAN 15, 1990    20:19
System      NI      DP
-----
          D      D      S
A A F L L P T  A   L O A Y E   Y
L C E L O L L  T   C O O I E E   T C N
M O L B C B B  A   V S F S L R   A A C
-----
* - - - - -   - - * - - - -   * * *
```



NOTE

The above illustration shows status for a HSSI data port. If you are using the V.35/EIA-530 data port, the “DP” status column displays the status of DTR, DCD, and CTS.

Column	Description
System	
ALM	An alarm condition exists.
ACO	The Alarm Cut Off (ACO) switch has been pressed to reset the external Alarm Relay. The alarm condition may still exist as indicated by the ALM column.
FEL	The IDSU has sent code to set a remote loopback in the far-end device. (The loopback has not necessarily been verified.)
LLB	The IDSU is set in a line loopback.
LOC	The IDSU is set in a local loopback.
PLB	The IDSU is set in a payload loopback.
DTLB	The IDSU is set in a data terminal loopback.

Column	Description
NI (Network Interface)	
DATA	Data is being received at the network interface; no failure exists.
CV	A code violation has been received at the network interface in the previous second.
LOS	A loss of signal (LOS) condition exists at the network interface.
OOF	The receive signal at the network interface is out of frame (OOF).
AIS	An alarm indication signal (AIS) is being received at the network interface, indicating that a device upstream of the network interface is in LOS, OOF, or test mode.
YEL	A yellow (AFA) alarm is being received at the network interface, indicating a device upstream of the network interface is in an OOF or LOS alarm state on the near side.
EER	The errored second or unavailable second threshold for the network interface has been exceeded.
DP (Data Port)—HSSI	
TA	The DTE is ready to send and receive data.
CA	The IDSU is ready to send and receive data.
SYNC	If the data port transmit and receive clocks are set to subrates (i.e., rates lower than the maximum HSSI clock rate), a “-” in this column indicates that the data port is out of sync with far-end, resulting in an overflow or underflow condition. If the data port is in sync with the far-end, an “*” appears in the column. If the data port clocking is set to the maximum HSSI rate, an “*” always appears in the column.
DP (Data Port)—V.35/EIA-530	
DTR	The DTE is ready to send and receive data.
DCD &CTS	The IDSU is ready to send and receive data.

Troubleshooting tree

Bit errors received on the network port are the most common source of problems. The most common errors are:

- Wiring errors at the installation site
- Wrong type of wiring used for T3 or E3 line extension
- Incorrect configuration of equipment

The best troubleshooting method is to start with the most critical alarm, find its cause and fix it, and then turn to the next alarm. The following alarm list is arranged from most to least critical.

EQF

If you receive an equipment alarm...

The IDSU has failed its self-test. Call our Customer Support office at the numbers listed [“Who to call for assistance” on page 8](#).

NI LOS

If you receive a loss-of-signal condition at the network interface...

An NI LOS condition occurs when the DataSMART T3/E3 IDSU cannot detect a signal at its network interface. To troubleshoot for this condition:

- Make sure that you have correctly connected the cable between the DataSMART T3/E3 IDSU network interface port and your service provider’s equipment.
- If you built the cable on-site, check the cable connectors. A reversal of the transmit and receive pairs, or an open receive pair, can cause this condition.
- If the above appear to be okay, ask your service provider to test your network line and correct any errors found.

Refer to your *DataSMART T3/E3 IDSU Installation Guide* for instructions on how to properly connect the network cable.

NI OOF

If the incoming signal at the network interface is out-of-frame...

An out-of-frame condition occurs when the framing type you have configured for the network interface does not match the framing type of the incoming signal. To troubleshoot this condition:

- If your signal is T3, make sure framing is set to either C-Bit or M13 framing. If your signal is E3, make sure it is set to E3 framing. (See [“Specifying NI framing format” on page 41.](#))

A highly errored incoming signal can also cause an OOF condition.

NI AIS

If an alarm indication signal (AIS) is detected at the network interface...

An incoming AIS at the network interface indicates a problem with remote equipment on the T3 or E3 circuit. For example, the far-end equipment may not be connected or configured properly or is in a test mode, or the network interface unit (i.e., NIU or smart jack) may be in loopback, or your service provider may not have enabled your circuit yet. To troubleshoot this condition:

- Ask your service provider to trace the source of the AIS signal.

An NI AIS condition can also result from false alarms generated by pattern-sensitive fiber-optic multiplexing equipment on the T3 or E3 circuit. To troubleshoot this condition:

- Enable payload scrambling (**ESCRAM**) at each endpoint of the circuit. The unscrambled bit patterns may be causing the problem.

NI YEL

If incoming yellow is detected at the network interface...

An incoming yellow condition at the network interface indicates that the far-end equipment has a problem with the signal it is receiving from the DataSMART T3/E3 IDSU. To troubleshoot this condition:

- Check for an open, short, or wiring error in the cable between the DataSMART T3/E3 IDSU network interface port and your service provider’s network interface unit (i.e., NIU or smart jack). An open transmit pair can cause this condition.

NI EER

If an excessive error rate is detected at the network interface...

Excessive code violations are occurring in the network signal. There are several potential causes. To troubleshoot this condition:

- Make sure you haven't set too low a threshold for detecting errored seconds or unavailable seconds. A low setting increases error sensitivity. You might want to use the factory default threshold setting (see [page 37](#)).
- Make sure that you have correctly connected the cable between the DataSMART T3/E3 IDSU network interface port and your service provider's equipment. (Refer to your *DataSMART T3/E3 IDSU Installation Guide* for instructions on connecting the cable properly.)
- If you built the cable on-site, recheck the cable connectors. Loose or intermittent connections can cause an excessive error condition.
- Make sure the system clock is configured correctly.
- If all the above appear to be okay, ask your service provider to test your T3 or E3 line and correct any errors found.

DP NSYN

If the data port goes out of sync with the far-end...

If the data port is running at subrate clock speeds (i.e., slower than the maximum HSSI rates), it can experience an underflow or overflow condition if its transmit and receive clock rates are not synchronized with the far-end. To troubleshoot this condition:

- Synchronize the data port transmit clock rate with the receive clock rate at the far-end, and synchronize the data port receive clock rate with the transmit clock rate at the far-end.

Running the self-test diagnostics

The DataSMART T3/E3 IDSU runs through a diagnostic self-test when it powers up. You can also initiate the self-test from the command line at any time by entering **DST** at the prompt. If you activate self-test while the IDSU is in service, there will be a brief service interruption during the test.



CAUTION!

Do not initiate self-test when accessing the IDSU remotely through Telnet. Self-test will break your remote connection.

The self-test verifies the functions of DataSMART T3/E3 IDSU hardware circuitry. The results of self-test are indicated by the POWER/FAIL LED on the front of the unit. The POWER/FAIL LED initially turns red for approximately six seconds; it then turns green if the self-test passed. If the LED turns red and stays red, the self-test failed.

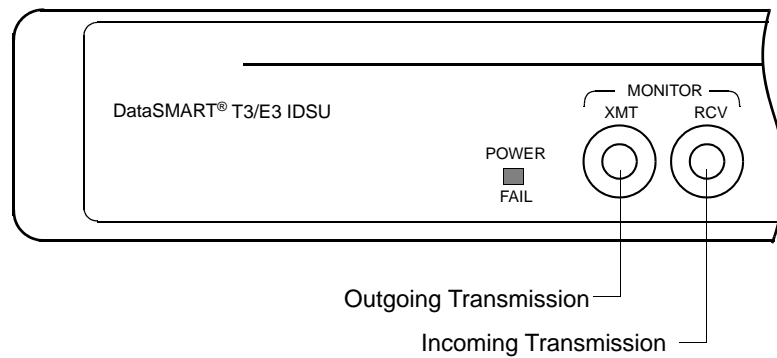
If self-test fails, the network LEDs on the front of the unit show which tests failed. If AIS is lit, the RAM read write test failed. If OOF is lit, the NVRAM tests failed. If LOS is lit, the EPROM has an invalid checksum.

When you execute the self-test, the DataSMART T3/E3 IDSU automatically resets any loopbacks. It does not clear the performance database, nor does it log you out of the system.

Using the network signal monitor jacks

The DataSMART T3/E3 IDSU provides two non-intrusive monitor jacks on its front panel. You can attach standard test equipment to these jacks and monitor incoming (RCV) and outgoing (XMT) T3 or E3 signal transmissions.

20dB signal loss/protection is provided to isolate the test equipment from the T3 or E3 circuit.

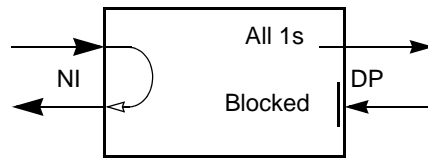


Using loopbacks

The DataSMART T3/E3 IDSU provides four loopbacks to support line segment testing. Line segment testing allows you to probe the T3 or E3 circuit to isolate where data flow is being corrupted or disrupted.

You can set all loopbacks locally, in your near-end device. You can also set the line and payload loopbacks remotely, in a far-end device, if you are using T3 C-Bit parity framing (T3 M13 and E3 framing do not support far-end loopbacks). Once you've set loopbacks, you can use test code insertion tools to test and monitor the line.

Line loopback

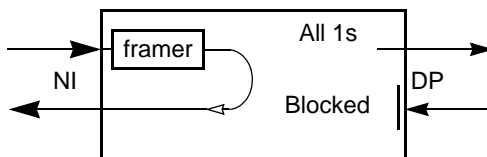


The line loopback allows the carrier (or a far-end device) to test the T3 or E3 signal at the DataSMART T3/E3 IDSU network interface. When set to line loopback, the IDSU loops the incoming signal back to the network. The signal minimally penetrates the IDSU and returns unaltered. It does not pass through the IDSU framer. The signal, including all code violation errors, is returned to the network unaltered and the carrier can test the looped signal for errors.

Once the line loopback is set, the incoming network signal is interrupted. CA (CTS and DCD) is de-asserted.

You can set the line loopback locally (see [page 74](#)), or you can set it remotely in a far-end device, if you are using T3 C-Bit parity framing (see [page 75](#)).

Payload loopback



By testing the T3 or E3 signal through a line loopback as described earlier, the carrier (or the far-end device) can determine if there are problems in the network line. What they cannot determine, however, is whether the problems are occurring on the receive or transmit side of the looped line. To further isolate the source of the problems to one side of the line or the other, you can use a payload loopback.

Payload loopback is the same as line loopback, except that the signal passes through the IDSU framer before being looped back. The framer strips out code violations but does not alter the payload data.

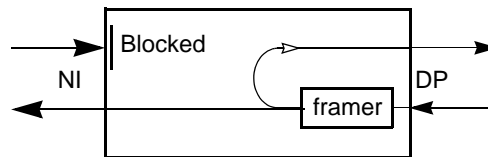
The condition of the returned signal indicates the cause of the problem:

- The line is okay if the returned signal contains no errors.
- The problem is usually on the transmit side of the line (as viewed from the carrier) if the returned signal contains pattern bit errors, but no code violations.
- The problem is on the receive side of the line (as viewed from the carrier) if the returned signal contains code violations, since they were introduced after the signal went through the IDSU framer.
- The problem may be on both the transmit side or the receive side if the returned signal contains pattern bit errors and code violations.
- The problem is probably a remote clock slip if the returned signal contains bursty pattern bit errors, but no code violations.

Once the payload loopback is set, the incoming network signal is interrupted. CA (CTS and DCD) is de-asserted.

You can set the payload loopback locally at the request of the carrier or a far-end site (see [page 74](#)), or you can set it remotely in a far-end device, if you are using T3 C-Bit parity framing (see [page 75](#)).

Local loopback



TIP

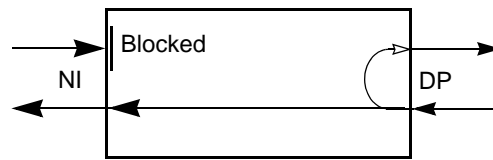
The local loopback is similar to a “hard” loopback set at the network interface.

The local loopback allows you to test data transmission from the DTE to the data port. This loopback allows maximum penetration of the data port. The data port receives the bit stream from the DTE, passes the signal through its framer, then loops it back to the DTE. By attaching a DTE device capable of monitoring the looped signal, you can verify the quality of the returned signal.

When the IDSU is set to local loopback, the outgoing signal at the network interface is interrupted. The IDSU outputs framed DTE data at the network interface.

You can only set a local loopback in your local IDSU (see [page 74](#)). You cannot set it remotely.

Data terminal loopback



Typically, you use the data terminal loopback to verify the cabling between the data port and the attached DTE device. You can also monitor the looped signal for errors at the DTE.

The data terminal loopback allows you to loop the incoming signal at a data port. When set in this loopback, the DataSMART T3/E3 IDSU loops the incoming signal back to the DTE device sending the signal. The signal minimally penetrates the DataSMART T3/E3 IDSU and is returned to the DTE device unaltered.

Setting and resetting loopbacks in your local device

You can set and reset loopbacks in your local device from the command line or using the front-panel thumbwheel switch. Only one loopback, either local or remote, may be set at one time. Remote loopbacks are only available in T3 C-Bit parity mode. You cannot set a loopback if another loopback is already active.

NOTE

A far-end device can set your IDSU to line or payload loopback by sending standard line loopback set and reset code.

Using the command line

The figure below illustrates the Local Maintenance menu. You use the commands in this menu to set or reset loopbacks in your local device. You must have super-user, configuration, or maintenance privileges.

local loopback commands —

```
LOCAL MAINTENANCE MENU

SLA / RLA - Set/Reset Local Alarm Relay

SLL      - Set the Line Loopback
SPL      - Set the Payload Loopback
SLO      - Set the Local Loopback
SDT      - Set the Data Terminal Loopback

RLB      - Reset Loopbacks

DST      - Do Self Test (Data Path Disruptive)

LM>
```

SLL Set a line loopback
SPL Set a payload loopback
SLO Set a local loopback
SDT Set a data terminal loopback

To reset a loopback in your local DataSMART T3/E3 IDSU, enter **RLB**.

Using the front-panel thumbwheel switch

You can set loopbacks in the local IDSU by using the IDSU's front-panel switch. Rotate the thumbwheel switch to the appropriate setting, then press the ACTV button.

Switch setting...	For...
4	LLB—Line loopback
5	PLB—Payload loopback
6	LOC—Local loopback
7	DTLB—Data terminal loopback

To reset the loopback, rotate the switch to 0 (RST) and press the ACTV button.

Setting and resetting loopbacks remotely (T3 C-Bit framing only)

You can set remote loopbacks if your network interface is set to T3 C-Bit parity framing. T3 M13 and E3 framing do not support remote loopbacks.

You can set a line or payload remotely, in a far-end device. Only one loopback may be set at one time. You cannot set a loopback if another loopback is already active.

Using the command line

The figure below illustrates the Remote Maintenance menu. You use the commands listed in this menu to set and reset remote loopbacks. You must have super-user, configuration, or maintenance privileges.

```
REMOTE MAINTENANCE MENU

SRL      - Set Remote Line Loopback
SRP      - Set Remote Payload Loopback

RLB      - Reset Remote Loopback

RM>
```

SRL Set a remote line loopback

SRP Set a remote payload loopback

To reset a remote loopback, enter **RST1**.

Using the front-panel thumbwheel switch

You can also set loopbacks in a remote device by using the IDSU's front-panel switch. Rotate the thumbwheel switch to the appropriate setting, then press the ACTV button.

Switch setting...	For...
1	RLLB—Remote line loopback
2	RPLB—Remote payload loopback

To reset the loopback, rotate the switch to 0 (RST) and press the ACTV button.

7

Using Telnet and SNMP

You can establish a SLIP interface connection through either the DCE or DTE control port of the DataSMART T3/E3IDSU. Through SLIP, you can:

- Telnet into the IDSU and access the normal user interface just as if you had logged in with a terminal
- Use an SNMP management system to access the supported MIB objects

When using a SLIP interface, you specify the control port for the interface via the **DCE** or the **DTE** command. You must disable alarm generation at this port by entering the **DAM** command. Alarms are output to the SLIP interface as traps.

This chapter describes how to enable the SLIP interface, and set up the IDSU for Telnet and SNMP access.

Enabling SLIP and specifying local IP information

The commands for enabling the SLIP interface and for setting up IP addressing are listed in the TCP/IP Configuration menu. To view this menu, enter **TCP** at the prompt.

```
TCP/IP CONFIGURATION MENU

SLADDR:<ipaddr>    - Set SLIP IP Address
SLMASK:<ipaddr>    - Set SLIP IP Subnet Mask
ESLIP/DSLIP        - Enable/Disable SLIP interface

IPR:<ipaddr>       - Set Default Router's IP Address
                   <ipaddr> = n.n.n.n, n = 0 .. 255 (decimal)
TPW:<str>          - Set Telnet Password
                   <str> = 1 to 20 chars, * = disable

TCPV               - View TCP/IP Configuration

TCP>
```

Viewing the current settings

Before changing any TCP/IP parameters, you may want to look at the current settings. You do this by executing the **TCPV** command. This command displays the View TCP/IP Configuration screen.

```
View TCP/IP Configuration

Interface      IP Address      Subnet mask
-----
SLIP Enable    198.26.27.1     255.255.255.0

Telnet Password
-----
kentrox

Default Router
-----
198.26.27.2

TCP>
```

Field	Description
Interface	This field shows you whether or not SLIP is enabled. (Alarm generation must be disabled (DAM) before SLIP is enabled.)
IP Address	This field tells you the IP address currently assigned to the IDSU.
Subnet mask	This field tells you the subnet mask of the local network to which the IDSU is connected.
Telnet Password	This field tells you the current Telnet password.

Setting the IP address and subnet mask

Field	Description
Default Router	This field tells you the IP address of the local network's default router. The default router must be on the same subnet as the IDSU.

An IP address and subnet mask are necessary for the IDSU to communicate with other equipment on the its local LAN network (for example, to communicate with a terminal connected via SLIP).

The IP address is a 32-bit binary address, typically written in dotted decimal notation: xxx.xxx.xxx.xxx. The bit settings identify two parameters: the local network value and the unique host value for the IDSU on that network.

The subnet mask (also 32-bits written in dotted decimal notation) determines which bits within the IP address define the network and which bits define the host (or IDSU). A 1 in a mask bit location means the corresponding bit in the IP address is part of the network value; a 0 means the corresponding bit is part of the host value. A standard subnet mask is 255.255.255.0, which specifies that the first 24 bits of the IP address define the network value, and the last 8 bits define the host value. For example, with a subnet mask of 255.255.255.0, the following IP address breaks down as follows:

198.126.27.2	
network	host

If you do not know what values you should use for the IP address and subnet mask, ask your system administrator.

You set the IP address and subnet mask by using the **SLADDR** and **SLMASK** commands, respectively. You must have super-user or configuration privileges. The command syntax is:

SLADDR:*ipaddr*

SLMASK:*ipaddr*

ipaddr Specify the IP address using dotted decimal notation (xxx.xxx.xxx.xxx).

Enabling/disabling SLIP

You must enable the SLIP interface. Before doing so specify the interface being used by entering either **DCE** or **DTE**, then disable alarm generation by entering **DAM**.



NOTE

Specify the IP address and subnet mask before enabling SLIP.

ESLIP Enable SLIP

DSLIP Disable SLIP

You can also disable the SLIP interface by setting the front-panel thumbwheel to 8 and pressing both the ACTV and ACO push-buttons for 2.5 seconds.

Setting the default router

You should always set up a default router for the IDSU if you plan to access the unit from a host whose IP address is on a different subnet (network) than the IDSU. When accessed by a host on a different subnet, the IDSU sends responses to the default router. The default router then routes the responses to the appropriate subnet.

The default router must be on the same subnet as the IDSU.

You set the default router by using the **IPR** command. You must have super-user or configuration privileges. The command syntax is:

IPR:*ipaddr*

ipaddr Specify the IP address of the default router using dotted decimal notation (*xxx.xxx.xxx.xxx*).

Setting the Telnet password

Telnet lets you remotely log into the IDSU and access its standard user interface, via the SLIP connection. When logging in via Telnet, you are prompted for a Telnet password. This password is not related to any other password set for the IDSU. The Telnet password is composed of 1 to 20 printable ASCII characters.

No default password exists; you must enter one using the **TPW** command. You must have super-user or configuration privileges.

The command syntax is:

TPW:*str*

str Enter the Telnet password using 1 to 20 printable characters.



NOTE

*It is possible to enter the command: **TPW:**<space>. This creates a Telnet password that is a single space. This password cannot be entered from a Telnet client, and will therefore cut off Telnet access to the IDSU. The only way to fix this problem is to access the IDSU through its other control port and change the Telnet password.*

Specifying the SNMP configuration

Once you've set up the SLIP interface and IP addressing, you can enable SNMP access. In most cases, the only additional configuration is adding network managers to the list of recipients of IDSU SNMP traps. You may also want to modify the SNMP community strings being used by the IDSU if your management station does not support the standard defaults.

To view the SNMP Configuration menu, enter **SNMP** at the prompt.

```
SNMP CONFIGURATION MENU

RCS:<str>      - Set SNMP Read Community String, str = 1 to 20 chars
WCS:<str>      - Set SNMP Write Community String, str = 1 to 20 chars
TCS:<str>      - Set SNMP Trap Community String, str = 1 to 20 chars
                <str> = * to delete a community string

ADD:T:<ipaddr> - Add address to SNMP trap list
DEL:T:<ipaddr> - Delete address from SNMP trap list
                <ipaddr> = n.n.n.n, n = 0 .. 255 (decimal)
                <ipaddr> = * in DEL command to delete all addresses

ESNMP / DSNMP - Enable/Disable The SNMP Agent
SNMPV         - View SNMP Configuration

SNMP>
```

Viewing the current settings

Before changing any parameters, you may want to look at the current settings for SNMP. You do this by entering **SNMPV** at the prompt.

```
View SNMP Configuration

Write Community String  Read Community String  Trap Community String
-----
private                public                 public

SNMP Agent
-----
Enable

Trap Destination IP Address List
-----
198.26.27.5

SNMP>
```

Field	Description
Write Community String Read Community String Trap Community String	These fields list the current SNMP community strings.
SNMP Agent	This field specifies whether SNMP access is enabled or disabled.

Field	Description
Trap Destination IP Address List	This field displays the IP hosts to which the IDSU sends traps.

Setting SNMP community strings

SNMP community strings are like passwords. Every SNMP packet has a community string (read, write, or trap, depending on the kind of SNMP packet). The packet's community string must match the community string on the SNMP agent/manager receiving the SNMP packet or it will be discarded.

The SNMP community strings all consist of 1 to 20 printable ASCII characters. These strings are case-sensitive.

The IDSU ships with the standard default values for the community strings.

Using the WCS command

You configure the SNMP write community string by using the **WCS** command. The write community string is used when an SNMP-set packet is received. The command syntax is:

WCS:*str*

str A string of 1 to 20 printable ASCII characters. This string is case-sensitive.

default private

Using the RCS command

You configure the SNMP read community string by using the **RCS** command. The read community string is used when an SNMP-get or SNMP-getnext packet is received. The command syntax is:

RCS:*str*

str A string of 1 to 20 printable ASCII characters. This string is case-sensitive.

default public

Using the TCS command

You configure the SNMP trap community string by using the **TCS** command. The trap community string is used when an SNMP trap is received. The command syntax is:

TCS:*str*

str A string of 1 to 20 printable ASCII characters. This string is case-sensitive.

default public

Configuring SNMP trap hosts

SNMP traps are sent to configured trap hosts when alarm conditions occur. Up to 25 unique IP addresses can be entered into the trap host destinations list.

Using the ADD command

You add an IP address to the SNMP trap destinations list by using the **ADDT** command. The command syntax is:

ADD:T:ipaddr

ipaddr Specify the IP address that you want SNMP traps to be sent to.

Using the DELT command

You remove an IP address from the SNMP trap destinations list by using the **DELT** command. The command syntax is:

DEL:T:ipaddr

ipaddr Specify the IP address that you want to remove from the SNMP traps destination list. Use "*" to delete all the entries in the SNMP trap destination list.

Enabling/disabling the SNMP agent

The SNMP agent is the heart of the IP host of the IDSU. For SNMP operations to work, SNMP must be enabled. The default setting for the SNMP agent is disabled.

You enable the SNMP agent by entering the **ESNMP** command. You disable the SNMP agent by using the **DSNMP** command.

Specifying source address screening configuration

The IDSU is secured from unauthorized remote access by the Telnet password protection and by SNMP community strings. For additional security you can configure the IDSU to screen out incoming packets based on the IP source address.

The commands for configuring source address screening are listed below (enter **SCREEN** to see this display).

```

SOURCE ADDRESS SCREENING MENU

SSA:<c>          - Set packet Screening via Source Address
                  c = I (IP Addr) or N (None)
ADD:I:<ipaddr>   - Add address to Screening tables
DEL:I:<ipaddr>   - Delete address from Screening tables
                  <ipaddr> = n.n.n.n, n = 0 .. 255 (decimal)
                  <addr> = * in DEL command to delete all addresses

SCREENV         - View Screening Tables

SCREEN>
```

Viewing the current settings

Before changing any parameters, you may want to look at the current settings. You do this by executing the **SCREENV** command. This command displays the View Address Screening display.

```

View Address Screening

IP Address Screening
-----
Enable

IP Source Address Table
-----
192.228.59.2      192.228.60.4      192.228.60.5      192.228.60.10
198.26.27.9

SCREEN>
```

Field	Description
IP Address Screening	This field indicates whether IP source address screening is enabled or disabled.
IP Source Address Table	This field displays the IP addresses to which the IDSU will respond.

Enabling/disabling address screening

You enable or disable address screening by using the **SSA** command. You must have super-user or configuration privileges.

SSA:*c*

c Enter **I** to enable address screening, enter **N** to disable it.

Adding a host to the address screening list

You add an address to a screening list using the **ADD** command. The command syntax is:

ADD:*I:ipaddr*

ipaddr Specify the IP address of the host you want added to the list. Use dotted decimal notation.

Deleting a host from the address screening lists

You delete an address from a screening list by using the **DEL** command. The command syntax is:

DEL:*I:ipaddr*

ipaddr Specify the IP address of the host you want deleted from the list. Use dotted decimal notation. Enter * to delete all addresses from the list.

Traps & MIBs

The DataSMART T3/E3 IDSU supports the following standard traps:

- Link-up
- Link-down
- Cold-start

The DataSMART T3/E3 IDSU supports the following MIBs. See Chapter 8 for a complete listing.

- MIB II (RFC 1213)
- DS3/E3 MIB (RFC 1407)

8

Quick Reference

This chapter contains:

- A listing of all menus and commands available through the command-line interface
- A complete listing of DataSMART T3/E3 IDSU specifications

Command-line menus and commands

The command-line interface provides fourteen “help” menus. These menus group the various commands by function and describe the use and syntax of each command.

To display a menu, simply enter the acronym correlating to the menu title.

Main menu (MM)

```
DataSMART T3/E3 IDSU Version 3.22 Copyright (c) 1992-1995 Kentrox
ADDRESS: 00:00:000 NAME: PORTLAND,OR

MM - Main Menu
SS - Status Menu
R - Performance Report Menu
PE - Password Entry Menu

LM - Local Maintenance Menu
RM - Remote Maintenance Menu

AC - Alarm Configuration Menu
CC - Control Port Configuration Menu
NC - NI Configuration Menu
PC - Password Configuration Menu
SC - System Configuration Menu
TCP - TCP/IP Configuration Menu
SNMP - SNMP Configuration Menu
SCREEN - Source Address Screening

^D - Logout
^D<xx>:<yy>:<zzz>^E - Address Another Unit

MM>
```

System menu (SS)

```
STATUS MENU

SSV - View System Setup
S - System Status Screen Command

ACO - Alarm Cut Off

SS>
```

Reports menu (R)

```
PERFORMANCE REPORT MENU

UNSR / UNLR - User NI Short/Long Performance Report
FESR / FELR - Far End PRM Data Short/Long Performance Report
SDLR        - Subrate Data Long Performance Report

NSR         - User NI Statistical Report
AHR        - Alarm History Report

PL:<n>      - Page Length, n = 20 .. 70, (P - Page Break) (V - View)

R >
```

Password Entry menu (PE)

```
PASSWORD ENTRY MENU

EPS:<password> - Enter Password
                password = 6 to 12 characters

PEV          - View Access Privileges
PUV          - View User Access Privilege

PE>
```

Local Maintenance menu (LM)

```
LOCAL MAINTENANCE MENU

SLA / RLA - Set/Reset Local Alarm Relay

SLL       - Set the Line Loopback
SPL       - Set the Payload Loopback
SLO       - Set the Local Loopback
SDT       - Set the Data Terminal Loopback

RLB       - Reset Loopbacks

DST       - Do Self Test (Data Path Disruptive)

LM>
```

Remote Maintenance menu (RM)

```
REMOTE MAINTENANCE MENU

SRL      - Set Remote Line Loopback
SRP      - Set Remote Payload Loopback

RLB      - Reset Remote Loopback

RM>
```

Alarm Configuration menu (AC)

```
ALARM CONFIGURATION MENU

EAR / DAR      - Enable/Disable Alarm Relay
EAM / DAM      - Enable/Disable Alarm Messages
EUM / EMM      - User/Manager Alarm Message Format
DIR / DDD      - Direct/Dialout Alarm Message Output
EMS:<str>      - Enter Modem String, str = AT command(s)

EYL / DYL      - Enable/Disable YELLOW Activating the Alarm
EAI / DAI      - Enable/Disable AIS Activating the Alarm
EST:<n>        - Errored Second Threshold, n = 0 .. 900
UST:<n>        - Unavailable Second Threshold, n = 0 .. 900

ACV           - View Alarm Configuration

AC>
```

Control Port Configuration menu (CC)

```
CONTROL PORT CONFIGURATION MENU

EE / DE      - Enable/Disable Character Echo

CCV          - View Control Port Configuration

CC>
```

NI Configuration menu (NC)

```
NI CONFIGURATION MENU

NM13 / NCBT / NE3 - T3 M13, T3 C-Bit Parity, or E3 NI Framing Format
NLO / NHI         - Low/High NI Transmit Output Level
LBO:<IN or OUT>  - Sets the transmit Line Build Out to be IN or OUT

NCV               - View NI Configuration

NC>
```

Password Configuration menu (PC)

```
PASSWORD CONFIGURATION MENU

APS:<access>:<password> - Add Password
                        access  = SA - Super User
                                CA - Configuration
                                MA - Maintenance
                        password = 6 to 12 characters

DPS:<password>         - Delete Password

PCV                   - View Password Configuration

PC>
```

System Configuration menu (SC)

```
SYSTEM CONFIGURATION MENU

SD:<mmm>,<dd>,<yy> - Set Date
ST:<hh>:<mm> - Set Time
SN:<id> - Set Name
SA:<xx>:<yy>:<zzz> - Set the Unit's Address to slot:shelf:group
EFP / DFP - Enable/Disable Front Panel Operation
DCE / DTE - DCE/DTE is the Alarm Output Port
CLK:<src> - Clock Source, src = I (Internal), L (Looped)
DSUCLK:<xx.x>,<yy.y> - Sets DSU data port clock (direction is NI)
                    xx.x = transmit, yy.y = receive
HSSI / V35 / EIA530 - Select data port as HSSI, V.35 or EIA-530
ESCRAM/DSCRAM - Enable/Disable Scrambling on the DSU Data Port
ZALL - Zero All Counters used in User Reports
WYV - What's Your Version
RSD - Reset Unit to Dip Switch Defaults
SCV - View System Configuration

SC>
```

TCP/IP Configuration menu (TCP)

```
TCP/IP CONFIGURATION MENU

SLADDR:<ipaddr> - Set SLIP IP Address
SLMASK:<ipaddr> - Set SLIP IP Subnet Mask
ESLIP/DSLIP - Enable/Disable SLIP interface

IPR:<ipaddr> - Set Default Router's IP Address
              <ipaddr> = n.n.n.n, n = 0 .. 255 (decimal)
TPW:<str> - Set Telnet Password
           <str> = 1 to 20 chars, * = disable

TCPV - View TCP/IP Configuration

TCP>
```

SNMP Configuration menu (PC)

```
SNMP CONFIGURATION MENU

RCS:<str>          - Set SNMP Read Community String, str = 1 to 20 chars
WCS:<str>          - Set SNMP Write Community String, str = 1 to 20 chars
TCS:<str>          - Set SNMP Trap Community String, str = 1 to 20 chars
                   <str> = * to delete a community string

ADD:T:<ipaddr>     - Add address to SNMP trap list
DEL:T:<ipaddr>     - Delete address from SNMP trap list
                   <ipaddr> = n.n.n.n, n = 0 .. 255 (decimal)
                   <ipaddr> = * in DEL command to delete all addresses

ESNMP / DSNMP     - Enable/Disable The SNMP Agent
SNMPV             - View SNMP Configuration

SNMP>
```

Source Address Screening menu (SCREEN)

```
SOURCE ADDRESS SCREENING MENU

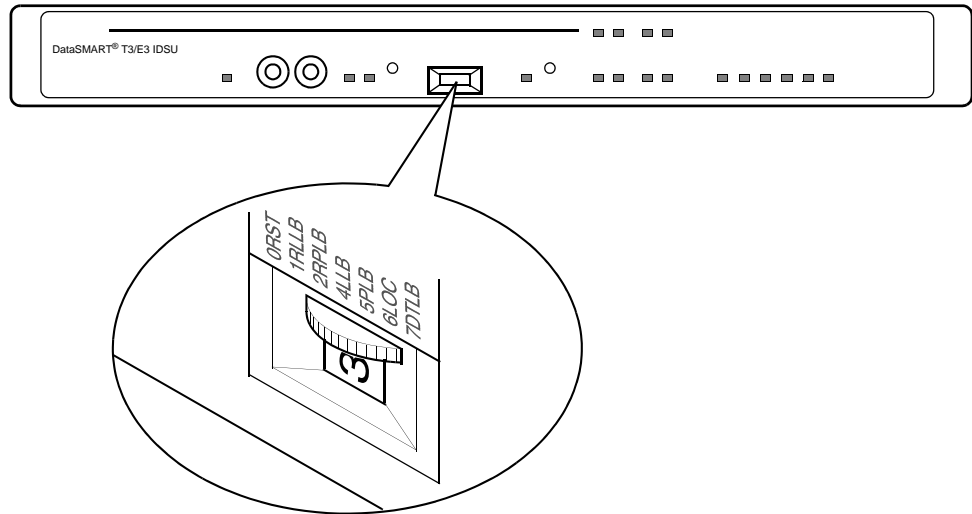
SSA:<c>           - Set packet Screening via Source Address
                   c = I (IP Addr) or N (None)
ADD:I:<ipaddr>    - Add address to Screening tables
DEL:I:<ipaddr>    - Delete address from Screening tables
                   <ipaddr> = n.n.n.n, n = 0 .. 255 (decimal)
                   <addr> = * in DEL command to delete all addresses

SCREENV          - View Screening Tables

SCREEN>
```

Front-panel thumbwheel switch

The front-panel thumbwheel switch allows you to set local and remote loopbacks. It also lets you reset the unit to factory defaults, overriding any configuration edits made previously.



The following table describes the switch settings. To activate a setting, you must press either or both push-buttons. Each switch function has an equivalent command in the user interface. These equivalents are listed in the table. Refer to your user's guide for information about the commands.



NOTE

Remote loopbacks can only be set if the network interface is T3 C-bit parity.

Set the thumbwheel to...	Push...	The following action results...
0 (RST) cmmnd equivalent= RLB	ACTV	Resets any active remote or local loopback.
1 (RLLB) cmmnd equivalent= SRL	ACTV	Sets a remote line loopback at the far-end.
2 (RPLB) cmmnd equivalent= SRP	ACTV	Sets a remote payload loopback at the far-end.
3	ACTV and ACO; hold for 3 seconds	Resets the unit to factory defaults. Control port baud rate and other terminal communication settings are set to internal DIP switch values.
4 (LLB) cmmnd equivalent= SLL	ACTV	Sets a line loopback at the near-end.

Set the thumbwheel to...	Push...	The following action results...
5 (PLB) cmmd equivalent= SPL	ACTV	Sets a payload loopback at the near-end.
6 (LOC) cmmd equivalent= SLO	ACTV	Sets a local loopback at the near-end.
7 (DTLB) cmmd equivalent= SDT	ACTV	Sets a data terminal loopback at the near-end.
8	ACTV and ACO	Disables the SLIP connection.
9	ACTV and ACO	Resets the IDSU device address to 00:00:000.

Specifications

Table 6—Environmental Specifications

	Parameter	Specification
Temperature	Storage	-20°C to 66°C (5% to 95% RH)
	Operating	0°C to 50°C (5% to 95% RH, non-condensing)
Powering	AC Input range	85 to 265 VAC, 47 to 63 Hz (24 W nominal, 30 W maximum)
	DC input range	36 to 75 VDC (22 W nominal, 25 W maximum)
	Power interruptions	Loss of power does not damage the unit.

Table 7—Electrical interface specifications - T3 Network Interface

	Parameter	Specification
Common	Line rate	Internal clock: 44.736 Mbps +/- 20 ppm Looped clock: output line rate follows input line rate
	Line Code	B3ZS Per TR-TSY-000499, section 9.5.2 and CCITT G.703, Annex A.1
	Line Impedance	75 ohms +/- 5% Per TR-TSY-000499, section 9.5.4
	Framing Format	M13, per ANSI T1.107-1088, or C-bit parity, per ANSI T1.107a-1990
Input Only	Input Signal	+6.2dBm to -11.7dBm
	Interfering Tone	Recovers T3 signals with an interfering tone as per CCITT G.703, section 8.3.4
	Input Jitter Tolerance	Per TR-TSY-000499, section 7.3.1, for category II equipment
Output Only	Output Level	0.36 to 0.85 V (peak) at DS3 cross-connect Per TR-TSY-000499, section 9.5.6
	Output Signal	DSX-3, T3 High (selectable)
	Line Build Out	Line build-out selectable for short cables
	Jitter Generation	Within ANSI T1.404-1989, section 5.8.2, standard
Network Interface Connector	(2) 75 ohm BNC female jacks	RCV (IN) and XMT (out)
Network Jacks	(2) BNC jacks	Receive and transmit signal monitoring, at or below 20dB output level.

Table 8—Electrical interface specifications - E3 Network Interface

	Parameter	Specification
Common	Line rate	Internal clock:34.368 Mbps +/- 20 ppm Per CCITT G.703, section 8.1 Looped clock: output line rate follows input line rate
	Line Code	HDB3 Per CCITT G.703, Annex A.1
	Line Impedance	75 ohms +/- 5% Per CCITT G.703, Table 8
	Return Loss	Calculated form Line Impedance: (CCITT G.703, section 8.3.3) 12 dB or greater, from 860 to 1720 KHz 18 dB or greater, from 1720 to 34368 KHz 14 dB or greater, from 34368 to 51550 KHz
	Framing Format	E3 Per CCITT G.751
Input Only	Input Signal	+6.2dBm to -11.7dBm
	Interfering Tone	Recovers E3 signals with an interfering tone as per CCITT G.703, section 8.3.4
	Input Jitter Tolerance	Per G.703, which in turn references G.823, section 3.1.1
Output Only	Output Level	Per G.703, Table 8, with mark equal to 1 +/- 0.1 V (peak-to-peak)
	Output Signal	E3
	Line Build Out	Line build-out selectable for short cables
	Jitter Generation	Within G.823, Table 1, standard
Network Interface Connectors	(2) 75 ohm BNC female jacks	RCV (IN) and XMT (out)
Network Jacks	(2) BNC jacks	Receive and transmit signal monitoring, at or below 20dB output level.

Table 9—Serial Control Port Specification

	Parameter	Specification
	Baud Rate	1200, 2400, 4800, 9600
	Electrical Interface	EIA-232D
Connector	DCE	EIA-561 module jack (8-pin)
	DTE	EIA-561 module jack (8-pin)

Table 10—Control port pin assignments

CCITT	Pin	Signal name	DTE	DCE
125	1	Ring Indicator (RI)	Input	Output
109	2	Rec Sign Det (DCD)	Input	Output
108.2	3	DTE Ready (DTR)	Output	Input
102	4	Signal GND	—	—
104	5	Received Data	Input	Output
103	6	Transmit Data	Output	Input
106	7	Clear To Send (CTS)	Input	Output
105	8	Request To Send (RTS)	Output	Input

Table 11—HSSI Data Port Interface Specification

Parameter	Specification
Bit Rates	T3: 1 to 35 MHz (0.5 MHz increments), 44.210 MHz E3: 1 to 24.5 MHz (0.5 MHz increments), 34.100 MHz
Max Bit Rates	T3: Gapped clock during M-frame overhead bits, at 44.210 Mbps +/- 20 ppm E3: Gapped clock during FAS, A, N overhead bits, at 34.100 Mbps +/- 20 ppm
Connector	HSSI
Electrical Interfaces	HSSI
Interface Type	DCE

Table 12—HSSI pin assignments

+ Pin	- Pin	Circuit name	Source
1	26	SG-Signal Ground	—
2	27	RT-Receive Timing	DCE
3	28	CA-DCE Available	DCE
4	29	RD-Receive Data	DCE
5	30	LC-Loopback circuit C	DCE
6	31	ST-Send Timing	DCE
7	32	SG-Signal Ground	—

Table 12—HSSI pin assignments (continued)

+ Pin	- Pin	Circuit name	Source
8	33	TA-DTE Available	DTE
9	34	TT-Terminal Timing	DTE
10	35	LA-Loopback circuit A	DTE
11	36	SD-Send Data	DTE
12	37	LB-Loopback circuit B	DTE
13	38	SG-Signal Ground	—
14, 15, 16, 17, 18	39, 40, 41, 42, 43	Reserved for future use.	DTE
19	44	SG-Signal Ground	—
20, 21, 22, 23, 24	45, 46, 47, 48, 49	Reserved for future use.	DCE
25	50	SG-Signal Ground	—

Table 13—V.35 Data Port Interface Specification

Parameter	Specification
Bit Rates	1.0 MHz to 8.0 MHz (0.5 MHz increments)
Connector	25-pin D connector, adaptable to V.35 or EIA-530 (EIA-449 or X.21 with adapters)
Electrical Interfaces	V.35 EIA-530, per ANSI/EIA-530-1987 X.25: EIA-530 (V.11, X.27 compatible)
Interface Type	DCE

Table 14—DB25D connector pin assignments for EIA-530

Pin	Designator CCITT/EIA	Circuit name	Source
1	—	Shield	—
2	(a) 103/BA	BA (A), Transmitted Data	DTE
3	(a) 104/BB	BB (A), Received Data A	DCE
4	(a) 105/CA	CA (A), Request To Send A (RTS)	DTE
5	(a) 106/CB	CB (A), Clear To Send A (CTS)	DCE

Table 14—DB25D connector pin assignments for EIA-530

Pin	Designator CCITT/EIA	Circuit name	Source
6	(a) 107/CC	CC (A), DCE Ready (DSR)	DCE
7	102/AB	AB, Signal Ground	—
8	(a) 109/CF	CF (A), Received Line Signal Detector	DCE
9	(b) 115/DD	DD (B), Receiver Signal Element Timing	DCE
10	(b) 109/CF	CF (B), Received Line Signal Detector	DCE
11	(b) 113/DA	DA (B), Transmit Signal Element Timing	DTE
12	(b) 114/DB	DB (B), Transmit Signal Element Timing	DCE
13	(b) 106/CB	CB (B), Clear To Send	DCE
14	(b) 103/BA	BA (B), Transmitted Data	DTE
15	(a) 114/DB	DB (A), Transmit Signal Element Timing	DCE
16	(b) 104/BB	BB (B), Received Data	DCE
17	(a) 115/DD	DD (A), Receiver Signal Element Timing	DCE
18	141/LL	LL, Local Loopback	DTE
19	(b) 105/CA	CA (B), Request To Send	DTE
20	108.2/CD	CD (A), DTE Ready	DTE
21	140/RL	RL, Remote Loopback	DTE
22	(b) 107/CC	CC (B), DCE Ready	DCE
23	(b) 108.2/CD	CD (B), DTE Ready	DTE
24	113/DA	DA (A), Transmit Signal Element Timing	DTE
25	142/TM	TM, Test Mode	DCE

Table 15—DB25D connector pin assignments for V.35

Pin	CCITT	Circuit name	Source
1	—	Protective GND	—
2	(a) 103	Tx Data A	DTE
3	(a) 104	Rx Data A	DCE
4	105	RTS	DTE
5	106	CTS	DCE
6	107	DSR	DCE

Table 15—DB25D connector pin assignments for V.35

Pin	CCITT	Circuit name	Source
7	102	Signal GND	—
8	109	Rec Line Sig Det (DCD)	DCE
9	(b) 115	Rx Timing B	DCE
10	—	No used	—
11	(b) 113	External clock B	DTE
12	(b) 114	Tx Timing B	DCE
13	—	Not used	—
14	(b) 103	Tx Data B	DTE
15	(a) 114	Tx Signal Timing A	DCE
16	(b) 104	Rx Data B	DCE
17	(a) 115	Rx Signal Timing A	DCE
18	141	LL, Local Loopback	DTE
19	—	Not used	—
20	108.2	DTR	DTE
21	140	RL, Remote Loopback	DTE
22	—	Not supported	—
23	—	Not used	—
24	(a) 113	External Clk A	DTE
25	142	TM, Test Mode	DCE

MIB II (RFC 1213) support

The system group

Object Name & OID	Access	Values	Description
sysDescr 1.3.6.1.2.1.1.1.0	read-only	DisplayString SIZE (0...255)	A textual description of this entity: "KENTROX DataSMART T3/E3".
sysObjectID 1.3.6.1.2.1.1.2.0	read-only	OBJECT IDENTIFIER	The vendor's authoritative identification of the network management subsystem contained in the entity. This value is ".iso.org.dod.internet.private.enterprises.adcKentrox.ktxProducts.3".
sysUpTime 1.3.6.1.2.1.1.3.0	read-only	TimeTicks	The time (in hundredths of a second) since the network management portion of the system was last reinitialized. It monotonically increases and tracks wall-clock time.
sysContact 1.3.6.1.2.1.1.4.0	read-write	DisplayString SIZE (0...255)	The textual identification of the contact person for this managed node, together with information on how to contact this person. This value can be "set", but it is not retained in the nonvolatile database.
sysName 1.3.6.1.2.1.1.5.0	read-write	DisplayString SIZE (0...255)	An administratively-assigned name for this managed node. Setting this value is the same as using the SN command. This value is stored in the nonvolatile memory.
sysLocation 1.3.6.1.2.1.1.6.0	read-write	DisplayString SIZE (0...255)	The physical location of this node (e.g., 'telephone closet, 3rd floor'). This value can be "set", but it is not retained in the nonvolatile database.
sysServices 1.3.6.1.2.1.1.7.0	read-only	INTEGER 0...127	A value that indicates the set of services that this entity primarily offers. The value is a sum. This sum initially takes the value zero. Then, for each layer, L, in the range 1 through 7, that this node performs transactions for, 2 raised to (L - 1) is added to the sum. For example, a node which performs primarily routing functions would have a value of 4 (2 ³⁻¹). In contrast, a node which is a host offering application services would have a value of 72 (2 ⁴⁻¹ + 2 ⁷⁻¹). Note that in the context of the Internet suite of protocols, values should be calculated accordingly: layer functionality 1 physical (e.g., repeaters) 2 datalink/subnetwork (e.g., bridges) 3 internet (e.g., IP gateways) 4 end-to-end (e.g., IP hosts) 7 applications (e.g., mail relays) The IDSU value is 2.

The interfaces group

Object Name & OID	Access	Values	Description
<i>ifNumber</i> 1.3.6.1.2.1.2.1.0	read-only	INTEGER	The number of IP interfaces (regardless of their current state) present on this system. The value for the IDSU is 1.
<i>ifTable</i> 1.3.6.1.2.1.2.2	not-accessible	SEQUENCE OF <i>IfEntry</i>	A list of interface entries. The number of entries is given by the value of <i>ifNumber</i> .
<i>ifEntry</i> 1.3.6.1.2.1.2.2.1	not-accessible	IfEntry	An interface entry containing objects at the subnetwork layer and below for a particular interface. An <i>ifEntry</i> includes the following objects: <i>ifIndex</i> <i>ifDescr</i> <i>ifType</i> <i>ifMtu</i> <i>ifSpeed</i> <i>ifPhysAddress</i> <i>ifAdminStatus</i> <i>ifOperStatus</i> <i>ifLastChange</i> <i>ifInOctets</i> <i>ifInUcastPkts</i> <i>ifInNUcastPkts</i> <i>ifInDiscards</i> <i>ifInErrors</i> <i>ifInUnknownProtos</i> <i>ifOutOctets</i> <i>ifOutUcastPkts</i> <i>ifOutNUcastPkts</i> <i>ifOutDiscards</i> <i>ifOutErrors</i> <i>ifOutQLen</i> <i>ifSpecific</i>
<i>ifIndex</i> 1.3.6.1.2.1.2.2.1.1.ifIndex	read-only	INTEGER	The <i>ifIndex</i> follows the definition given in RFC 1573: "A unique value, greater than zero, for each interface.". The value for the IDSU is 1.
<i>ifDescr</i> 1.3.6.1.2.1.2.2.1.2.ifIndex	read-only	DisplayString SIZE (0...255)	A textual string containing information about the interface. The IDSU constant value is "slip00".
<i>ifType</i> 1.3.6.1.2.1.2.2.1.3.ifIndex	read-only	INTEGER <i>slip</i> (28)	The type of interface, distinguished according to the physical/link protocol(s) immediately 'below' the network layer in the protocol stack. The IDSU always returns the value for SLIP (28).

Object Name & OID	Access	Values	Description
<i>ifMtu</i> 1.3.6.1.2.1.2.2.1.4.ifIn dex	read-only	INTEGER 1008	The size of the largest datagram which can be sent/received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface. The constant value for the IDSU is 1008.
<i>ifSpeed</i> 1.3.6.1.2.1.2.2.1.5.ifIn dex	read-only	GAUGE	The baud rate for the slip port: 9600, 4800, 2400, or 1200.
<i>ifPhysAddress</i> 1.3.6.1.2.1.2.2.1.6.ifIn dex	read-only	PhysAddress	The interface's address at the protocol layer immediately 'below' the network layer in the protocol stack. For interfaces that do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.
<i>ifAdminStatus</i> 1.3.6.1.2.1.2.2.1.7.ifIn dex	read-write	INTEGER <i>up(1)</i> ,	The desired state of the interface. The constant value for the IDSU is 1.
<i>ifOperStatus</i> 1.3.6.1.2.1.2.2.1.8.ifIn dex	read-only	INTEGER <i>up(1)</i>	The current operational state of the interface. The IDSU always returns a value of 1.
<i>ifLastChange</i> 1.3.6.1.2.1.2.2.1.9.ifIn dex	read-only	TimeTicks	The time value associated with the last issue of ESLIP, or the last interface change.
<i>ifInOctets</i> 1.3.6.1.2.1.2.2.1.10.ifI ndex	read-only	Counter	The total number of octets the slip interface has received as packets.
<i>ifInUcastPkts</i> 1.3.6.1.2.1.2.2.1.11.ifI ndex	read-only	Counter	The number packets received.
<i>ifInNUcastPkts</i> 1.3.6.1.2.1.2.2.1.12.ifI ndex	read-only	Counter	The IDSU always returns a value of 0.
<i>ifInDiscards</i> 1.3.6.1.2.1.2.2.1.13.ifI ndex	read-only	Counter	The number of bad packets received.
<i>ifInErrors</i> 1.3.6.1.2.1.2.2.1.14.ifI ndex	read-only	Counter	The IDSU always returns a value of 0.
<i>ifInUnknownProtos</i> 1.3.6.1.2.1.2.2.1.15.ifI ndex	read-only	Counter	The IDSU always returns a value of 0.

Object Name & OID	Access	Values	Description
<i>ifOutOctets</i> 1.3.6.1.2.1.2.2.1.16.ifIndex	read-only	Counter	The total number of octets counted in the outgoing slip packets.
<i>ifOutUcastPkts</i> 1.3.6.1.2.1.2.2.1.17.ifIndex	read-only	Counter	The total number of outgoing slip packets.
<i>ifOutNUcastPkts</i> 1.3.6.1.2.1.2.2.1.18.ifIndex	read-only	Counter	The IDSU always returns a value of 0.
<i>ifOutDiscards</i> 1.3.6.1.2.1.2.2.1.19.ifIndex	read-only	Counter	The IDSU always returns a value of 0.
<i>ifOutErrors</i> 1.3.6.1.2.1.2.2.1.20.ifIndex	read-only	Counter	The IDSU always returns a value of 0.
<i>ifOutQLen</i> 1.3.6.1.2.1.2.2.1.21.ifIndex	read-only	Gauge	The IDSU always returns a value of 0.
<i>ifSpecific</i> 1.3.6.1.2.1.2.2.1.22.ifIndex	read-only	OBJECT IDENTIFIER	This is 0.0 for the slip interface.

The IP group

Object Name & OID	Access	Values	Description
<i>ipForwarding</i> 1.3.6.1.2.1.2.4.1.0	read-write	INTEGER <i>forwarding</i> (1), <i>not-forwarding</i> (2)	The indication of whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. This value is always <i>not-forwarding</i> (2). The value can be set to 1, but it has no effect because the IDSU does not forward IP datagrams.
<i>ipDefaultTTL</i> 1.3.6.1.2.1.2.4.2.0	read-write	INTEGER	The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol.
<i>ipInReceives</i> 1.3.6.1.2.1.2.4.3.0	read-only	Counter	The total number of input datagrams received from interfaces, including those received in error.
<i>ipInHdrErrors</i> 1.3.6.1.2.1.2.4.4.0	read-only	Counter	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

Object Name & OID	Access	Values	Description
<i>ipInAddrErrors</i> 1.3.6.1.2.1.2.4.5.0	read-only	Counter	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
<i>ipForwDatagrams</i> 1.3.6.1.2.1.2.4.6.0	read-only	Counter	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. This value is always zero. The IDSU does not forward IP datagrams.
<i>ipInUnknownProtos</i> 1.3.6.1.2.1.2.4.7.0	read-only	Counter	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
<i>ipInDiscards</i> 1.3.6.1.2.1.2.4.8.0	read-only	Counter	The number of packets rejected because of IP address screening violations.
<i>ipInDelivers</i> 1.3.6.1.2.1.2.4.9.0	read-only	Counter	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
<i>ipOutRequests</i> 1.3.6.1.2.1.2.4.10.0	read-only	Counter	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in <i>ipForwDatagrams</i> .
<i>ipOutDiscards</i> 1.3.6.1.2.1.2.4.11.0	read-only	Counter	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in <i>ipForwDatagrams</i> if any such packets met this (discretionary) discard criterion.
<i>ipOutNoRoutes</i> 1.3.6.1.2.1.2.4.12.0	read-only	Counter	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in <i>ipForwDatagrams</i> that meet this 'no-route' criterion. Note that this includes any datagrams that a host cannot route because all its default gateways are down.
<i>ipReasmTimeout</i> 1.3.6.1.2.1.2.4.13.0	read-only	INTEGER	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
<i>ipReasmReqds</i> 1.3.6.1.2.1.2.4.14.0	read-only	Counter	The number of IP fragments received which needed to be reassembled at this entity.
<i>ipReasmOKs</i> 1.3.6.1.2.1.2.4.15.0	read-only	Counter	The number of IP datagrams successfully reassembled.

Object Name & OID	Access	Values	Description
ipReasmFails 1.3.6.1.2.1.2.4.16.0	read-only	Counter	The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
ipFragOKs 1.3.6.1.2.1.2.4.17.0	read-only	Counter	The number of IP datagrams that have been successfully fragmented at this entity.
ipFragFails 1.3.6.1.2.1.2.4.18.0	read-only	Counter	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.
ipFragCreates 1.3.6.1.2.1.2.4.19.0	read-only	Counter	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
ipAddrTable 1.3.6.1.2.1.2.4.20	not-accessible	SEQUENCE OF <i>IpAddrEntry</i>	The table of addressing information relevant to this entity's IP addresses.
ipAddrEntry 1.3.6.1.2.1.2.4.20.1	not-accessible	IpAddrEntry	The addressing information for one of this entity's IP addresses. An <i>ipAddrEntry</i> consists of the following objects: <i>ipAdEntAddr</i> <i>ipAdEntIfIndex</i> <i>ipAdEntNetMask</i> <i>ipAdEntBcastAddr</i> <i>ipAdEntReasmMaxSize</i>
ipAdEntAddr 1.3.6.1.2.1.2.4.20.1.1.ipAd EntAddr	read-only	IpAddress	The IP address to which this entry's addressing information pertains.
ipAdEntIfIndex 1.3.6.1.2.1.2.4.20.1.2.ipAd EntAddr	read-only	INTEGER	The index value that uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of <i>ifIndex</i> .
ipAdEntNetMask 1.3.6.1.2.1.2.4.20.1.3.ipAd EntAddr	read-only	IpAddress	The subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the host bits set to 0.
ipAdEntBcastAddr 1.3.6.1.2.1.2.4.20.1.4.ipAd EntAddr	read-only	INTEGER	The value of the least-significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value will be 1. This value applies to both the subnet and network broadcasts addresses used by the entity on this (logical) interface.
ipAdEntReasmMaxSize 1.3.6.1.2.1.2.4.20.1.5.ipAd EntAddr	read-only	INTEGER 0...65535	The size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface.

The IP Routing table

Object Name & OID	Access	Values	Description
ipRouteTable 1.3.6.1.2.1.2.4.21	not-accessible	SEQUENCE OF <i>IpRouteEntry</i>	This entity's IP Routing table.
ipRouteEntry 1.3.6.1.2.1.2.4.21.1	not-accessible	IpRouteEntry	A route to a particular destination. An <i>ipRouteEntry</i> consists of the following objects: <i>ipRouteDest</i> <i>ipRouteIfIndex</i> <i>ipRouteMetric1</i> <i>ipRouteMetric2</i> <i>ipRouteMetric3</i> <i>ipRouteMetric4</i> <i>ipRouteNextHop</i> <i>ipRouteType</i> <i>ipRouteProto</i> <i>ipRouteAge</i> <i>ipRouteMask</i> <i>ipRouteMetric5</i> <i>ipRouteInfo</i>
ipRouteDest 1.3.6.1.2.1.2.4.21.1.1.ipRouteDest	read-write	IpAddress	The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network management protocol in use.
ipRouteIfIndex 1.3.6.1.2.1.2.4.21.1.2.ipRouteDest	read-write	INTEGER	The index value which uniquely identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index is the same interface as identified by the same value of <i>ifIndex</i> .
ipRouteMetric1 1.3.6.1.2.1.2.4.21.1.3.ipRouteDest	read-write	INTEGER	The primary routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the route's <i>ipRouteProto</i> value. If this metric is not used, its value should be set to -1.
ipRouteMetric2 1.3.6.1.2.1.2.4.21.1.4.ipRouteDest	read-write	INTEGER	An alternate routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the route's <i>ipRouteProto</i> value. If this metric is not used, its value should be set to -1.
ipRouteMetric3 1.3.6.1.2.1.2.4.21.1.5.ipRouteDest	read-write	INTEGER	An alternate routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the route's <i>ipRouteProto</i> value. If this metric is not used, its value should be set to -1.
ipRouteMetric4 1.3.6.1.2.1.2.4.21.1.6.ipRouteDest	read-write	INTEGER	An alternate routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the route's <i>ipRouteProto</i> value. If this metric is not used, its value should be set to -1.

Object Name & OID	Access	Values	Description
ipRouteNextHop 1.3.6.1.2.1.2.4.21.1.7.ipRouteDest	read-write	IpAddress	The IP address of the next hop of this route. (In the case of a route bound to an interface which is realized via a broadcast media, the value of this field is the agent's IP address on that interface.)
ipRouteType 1.3.6.1.2.1.2.4.21.1.8.ipRouteDest	read-write	INTEGER <i>other</i> (1), <i>invalid</i> (2), <i>direct</i> (3), <i>indirect</i> (4)	<p>The type of route. Note that the values <i>direct</i>(3) and <i>indirect</i>(4) refer to the notion of direct and indirect routing in the IP architecture.</p> <p>Setting this object to the value <i>invalid</i>(2) has the effect of invalidating the corresponding entry in the <i>ipRouteTable</i> object. That is, it effectively disassociates the destination identified with said entry from the route identified with said entry. It is an implementation-specific matter as to whether or not the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant <i>ipRouteType</i> object.</p>
ipRouteProto 1.3.6.1.2.1.2.4.21.1.9.ipRouteDest	read-only	INTEGER <i>other</i> (1), <i>local</i> (2), <i>netmgmt</i> (3), <i>icmp</i> (4), <i>egp</i> (5), <i>ggp</i> (6), <i>hello</i> (7), <i>rip</i> (8), <i>is-is</i> (9), <i>es-is</i> (10), <i>ciscoIgrp</i> (11), <i>bbnSpfIgp</i> (12), <i>ospf</i> (13), <i>bgp</i> (14)	The routing mechanism via which this route was learned. Inclusion of values for gateway routing protocols is not intended to imply that hosts should support those protocols.
ipRouteAge 1.3.6.1.2.1.2.4.21.1.10.ipRouteDest	read-write	INTEGER	The number of seconds since this route was last updated or otherwise determined to be correct. Note that no semantics of 'too old' can be implied except through knowledge of the routing protocol by which the route was learned.
ipRouteMask 1.3.6.1.2.1.2.4.21.1.11.ipRouteDest	read-write	IpAddress	<p>Indicate the mask to be logical-ANDed with the destination address before being compared to the value in the <i>ipRouteDest</i> field. For those systems that do not support arbitrary subnet masks, an agent constructs the value of the <i>ipRouteMask</i> by determining whether the value of the correspondent <i>ipRouteDest</i> field belong to a class-A, B, or C network, and then using one of:</p> <p>mask network 255.0.0.0 class-A 255.255.0.0 class-B 255.255.255.0 class-C</p> <p>If the value of the <i>ipRouteDest</i> is 0.0.0.0 (a default route), then the mask value is also 0.0.0.0. It should be noted that all IP routing subsystems implicitly use this mechanism.</p>

Object Name & OID	Access	Values	Description
<i>ipRouteMetric5</i> 1.3.6.1.2.1.2.4.21.1.12.ipRouteDest	read-write	INTEGER	An alternate routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the route's <i>ipRouteProto</i> value. If this metric is not used, its value should be set to -1.
<i>ipRouteInfo</i> 1.3.6.1.2.1.2.4.21.1.13.ipRouteDest	read-only	OBJECT IDENTIFIER	A reference to MIB definitions specific to the particular routing protocol which is responsible for this route, as determined by the value specified in the route's <i>ipRouteProto</i> value. If this information is not present, its value should be set to the OBJECT IDENTIFIER { 0 0 }, which is a syntactically valid object identifier, and any conforming implementation of ASN.1 and BER must be able to generate and recognize this value.

Additional IP objects

Table 16—Additional IP objects

Object Name & OID	Access	Values	Description
<i>ipRoutingDiscards</i> 1.3.6.1.2.1.2.4.23.0	read-only	Counter	The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.

The ICMP group

Object Name & OID	Access	Values	Description
<i>icmpInMsgs</i> 1.3.6.1.2.1.2.5.1.0	read-only	Counter	The total number of ICMP messages that the entity received. Note that this counter includes all those counted by <i>icmpInErrors</i> .
<i>icmpInErrors</i> 1.3.6.1.2.1.2.5.2.0	read-only	Counter	The number of ICMP messages that the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
<i>icmpInDestUnreachs</i> 1.3.6.1.2.1.2.5.3.0	read-only	Counter	The number of ICMP Destination Unreachable messages received.
<i>icmpInTimeExcds</i> 1.3.6.1.2.1.2.5.4.0	read-only	Counter	The number of ICMP Time Exceeded messages received.
<i>icmpInParmProbs</i> 1.3.6.1.2.1.2.5.5.0	read-only	Counter	The number of ICMP Parameter Problem messages received.
<i>icmpInSrcQuenchs</i> 1.3.6.1.2.1.2.5.6.0	read-only	Counter	The number of ICMP Source Quench messages received.

Object Name & OID	Access	Values	Description
<i>icmpInRedirects</i> 1.3.6.1.2.1.2.5.7.0	read-only	Counter	The number of ICMP Redirect messages received.
<i>icmpInEchos</i> 1.3.6.1.2.1.2.5.8.0	read-only	Counter	The number of ICMP Echo (request) messages received.
<i>icmpInEchoReps</i> 1.3.6.1.2.1.2.5.9.0	read-only	Counter	The number of ICMP Echo Reply messages received.
<i>icmpInTimestamps</i> 1.3.6.1.2.1.2.5.10.0	read-only	Counter	The number of ICMP Timestamp (request) messages received.
<i>icmpInTimestampReps</i> 1.3.6.1.2.1.2.5.11.0	read-only	Counter	The number of ICMP Timestamp Reply messages received.
<i>icmpInAddrMasks</i> 1.3.6.1.2.1.2.5.12.0	read-only	Counter	The number of ICMP Address Mask Request messages received.
<i>icmpInAddrMaskReps</i> 1.3.6.1.2.1.2.5.13.0	read-only	Counter	The number of ICMP Address Mask Reply messages received.
<i>icmpOutMsgs</i> 1.3.6.1.2.1.2.5.14.0	read-only	Counter	The total number of ICMP messages that this entity attempted to send. Note that this counter includes all those counted by <i>icmpOutErrors</i> .
<i>icmpOutErrors</i> 1.3.6.1.2.1.2.5.15.0	read-only	Counter	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
<i>icmpOutDestUnreachs</i> 1.3.6.1.2.1.2.5.16.0	read-only	Counter	The number of ICMP Destination Unreachable messages sent.
<i>icmpOutTimeExcds</i> 1.3.6.1.2.1.2.5.17.0	read-only	Counter	The number of ICMP Time Exceeded messages sent.
<i>icmpOutParmProbs</i> 1.3.6.1.2.1.2.5.18.0	read-only	Counter	The number of ICMP Parameter Problem messages sent.
<i>icmpOutSrcQuenchs</i> 1.3.6.1.2.1.2.5.19.0	read-only	Counter	The number of ICMP Source Quench messages sent.
<i>icmpOutRedirects</i> 1.3.6.1.2.1.2.5.20.0	read-only	Counter	The number of ICMP Redirect messages sent. This object will always be zero.
<i>icmpOutEchos</i> 1.3.6.1.2.1.2.5.21.0	read-only	Counter	The number of ICMP Echo (request) messages sent.
<i>icmpOutEchoReps</i> 1.3.6.1.2.1.2.5.22.0	read-only	Counter	The number of ICMP Echo Reply messages sent.

Object Name & OID	Access	Values	Description
icmpOutTimestamps 1.3.6.1.2.1.2.5.23.0	read-only	Counter	The number of ICMP Timestamp (request) messages sent.
icmpOutTimestampReps 1.3.6.1.2.1.2.5.24.0	read-only	Counter	The number of ICMP Timestamp Reply messages sent.
icmpOutAddrMasks 1.3.6.1.2.1.2.5.25.0	read-only	Counter	The number of ICMP Address Mask Request messages sent.
icmpOutAddrMaskReps 1.3.6.1.2.1.2.5.26.0	read-only	Counter	The number of ICMP Address Mask Reply messages sent.

The TCP group

Object Name & OID	Access	Values	Description
tcpRtoAlgorithm 1.3.6.1.2.1.2.6.1.0	read-only	INTEGER <i>other</i> (1)	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets. The ID SU always returns a value of 1 (<i>other</i>).
tcpRtoMin 1.3.6.1.2.1.2.6.2.0	read-only	INTEGER 0	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. The ID SU always returns a value of 0.
tcpRtoMax 1.3.6.1.2.1.2.6.3.0	read-only	INTEGER 0	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. The ID SU always returns a value of 0.
tcpMaxConn 1.3.6.1.2.1.2.6.4.0	read-only	INTEGER 16	The limit on the total number of TCP connections the entity can support. The ID SU always returns a value of 16.
tcpActiveOpens 1.3.6.1.2.1.2.6.5.0	read-only	Counter	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
tcpPassiveOpens 1.3.6.1.2.1.2.6.6.0	read-only	Counter	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
tcpAttemptFails 1.3.6.1.2.1.2.6.7.0	read-only	Counter	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
tcpEstabResets 1.3.6.1.2.1.2.6.8.0	read-only	Counter	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
tcpCurrEstab 1.3.6.1.2.1.2.6.9.0	read-only	GAUGE	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.

Object Name & OID	Access	Values	Description
tcpInSegs 1.3.6.1.2.1.2.6.10.0	read-only	Counter	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs 1.3.6.1.2.1.2.6.11.0	read-only	Counter	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
tcpRetransSegs 1.3.6.1.2.1.2.6.12.0	read-only	Counter	The total number of segments retransmitted—that is, the number of TCP segments transmitted containing one or more previously transmitted octets.

The TCP connection table

Object Name & OID	Access	Values	Description
tcpConnTable 1.3.6.1.2.1.2.6.13	not-accessible	SEQUENCE OF <i>TcpConnEntry</i>	A table containing TCP connection-specific information.
tcpConnEntry 1.3.6.1.2.1.2.6.13.1	not-accessible	TcpConnEntry	Information about a particular current TCP connection. An object of this type is transient, in that it ceases to exist when (or soon after) the connection makes the transition to the CLOSED state. A <i>tcpConnEntry</i> consists of the following objects: <i>tcpConnState</i> <i>tcpConnLocalAddress</i> <i>tcpConnLocalPort</i> <i>tcpConnRemAddress</i> <i>tcpConnRemPort</i>
tcpConnState 1.3.6.1.2.1.2.6.13.1.1.tcpConnLocalAddress.tcpConnLocalPort.tcpConnRemAddress.tcpConnRemPort	read-write	INTEGER <i>closed</i> (1), <i>listen</i> (2), <i>synSent</i> (3), <i>synReceived</i> (4), <i>established</i> (5), <i>finWait1</i> (6), <i>finWait2</i> (7), <i>closeWait</i> (8), <i>lastAck</i> (9), <i>closing</i> (10), <i>timeWait</i> (11), <i>deleteTCB</i> (12)	The state of this TCP connection. The only value which may be set by a management station is <i>deleteTCB</i> (12). Accordingly, it is appropriate for an agent to return a <i>badValue</i> response if a management station attempts to set this object to any other value. If a management station sets this object to the value <i>deleteTCB</i> (12), then this has the effect of deleting the TCB (as defined in RFC 793) of the corresponding connection on the managed node, resulting in immediate termination of the connection. As an implementation-specific option, an RST segment may be sent from the managed node to the other TCP endpoint (note however that RST segments are not sent reliably).
tcpConnLocalAddress 1.3.6.1.2.1.2.6.13.1.2.tcpConnLocalAddress.tcpConnLocalPort.tcpConnRemAddress.tcpConnRemPort	read-only	IpAddress	The local IP address for this TCP connection. In the case of a connection in the listen state which is willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used.

Object Name & OID	Access	Values	Description
tcpConnLocalPort 1.3.6.1.2.1.2.6.13.1.3.tcpConnLocalAddress.tcpConnLocalPort.tcpConnRemAddress.tcpConnRemPort	read-only	INTEGER 0...65535	The local port number for this TCP connection. The IDSU returns the value of 23.
tcpConnRemAddress 1.3.6.1.2.1.2.6.13.1.4.tcpConnLocalAddress.tcpConnLocalPort.tcpConnRemAddress.tcpConnRemPort	read-only	IpAddress	The remote IP address for this TCP connection.
tcpConnRemPort 1.3.6.1.2.1.2.6.13.1.5.tcpConnLocalAddress.tcpConnLocalPort.tcpConnRemAddress.tcpConnRemPort	read-only	INTEGER 0...65535	The remote port number for this TCP connection.

Additional TCP objects

Object Name & OID	Access	Values	Description
tcpInErrs 1.3.6.1.2.1.2.6.14.0	read-only	Counter	The total number of segments received in error (e.g., bad TCP checksums).
tcpOutRsts 1.3.6.1.2.1.2.6.15.0	read-only	Counter	The number of TCP segments sent containing the RST flag.

The UDP group

Object Name & OID	Access	Values	Description
udpInDatagrams 1.3.6.1.2.1.2.7.1.0	read-only	Counter	The total number of UDP datagrams delivered to UDP users.
udpNoPorts 1.3.6.1.2.1.2.7.2.0	read-only	Counter	The total number of received UDP datagrams for which there was no application at the destination port.
udpInErrors 1.3.6.1.2.1.2.7.3.0	read-only	Counter	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
udpOutDatagrams 1.3.6.1.2.1.2.7.4.0	read-only	Counter	The total number of UDP datagrams sent from this entity.

The UDP listener table

Object Name & OID	Access	Values	Description
udpTable 1.3.6.1.2.1.2.7.5	not-accessible	SEQUENCE OF <i>udpEntry</i>	A table containing UDP listener information.
udpEntry 1.3.6.1.2.1.2.7.5.1	not-accessible	udpEntry	Information about a particular current UDP listener. A <i>udpEntry</i> consists of the following objects: <i>udpLocalAddress</i> <i>udpLocalPort</i>
udpLocalAddress 1.3.6.1.2.1.2.7.5.1.1.udpLocalAddress.udpLocalPort	read-only	IpAddress	The local IP address for this UDP listener. In the case of a UDP listener which is willing to accept datagrams for any IP interface associated with the node, the value 0.0.0.0 is used.
udpLocalPort 1.3.6.1.2.1.2.7.5.1.2.udpLocalAddress.udpLocalPort	read-only	INTEGER 0...65535	The local port number for this UDP listener.

The SNMP group

Object Name & OID	Access	Values	Description
snmplnPkts 1.3.6.1.2.1.2.11.1.0	read-only	Counter	The total number of Messages delivered to the SNMP entity from the transport service.
snmpOutPkts 1.3.6.1.2.1.2.11.2.0	read-only	Counter	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
snmplnBadVersions 1.3.6.1.2.1.2.11.3.0	read-only	Counter	The total number of SNMP Messages which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
snmplnBadCommunityNames 1.3.6.1.2.1.2.11.4.0	read-only	Counter	The total number of SNMP Messages delivered to the SNMP protocol entity which used a SNMP community name not known to said entity.
snmplnBadCommunityUses 1.3.6.1.2.1.2.11.5.0	read-only	Counter	The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message.
snmplnASNParseErrs 1.3.6.1.2.1.2.11.6.0	read-only	Counter	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP Messages.
snmplnTooBigs 1.3.6.1.2.1.2.11.8.0	read-only	Counter	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>tooBig</i> .

Object Name & OID	Access	Values	Description
snmplnNoSuchNames 1.3.6.1.2.1.2.11.9.0	read-only	Counter	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>noSuchName</i> .
snmplnBadValues 1.3.6.1.2.1.2.11.10.0	read-only	Counter	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>badValue</i> .
snmplnReadOnlys 1.3.6.1.2.1.2.11.11.0	read-only	Counter	The total number of valid SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>readOnly</i> . It should be noted that it is a protocol error to generate an SNMP PDU which contains the value <i>readOnly</i> in the error-status field, as such this object is provided as a means of detecting incorrect implementations of the SNMP.
snmplnGenErrs 1.3.6.1.2.1.2.11.12.0	read-only	Counter	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is <i>genErr</i> .
snmplnTotalReqVars 1.3.6.1.2.1.2.11.13.0	read-only	Counter	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
snmplnTotalSetVars 1.3.6.1.2.1.2.11.14.0	read-only	Counter	The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
snmplnGetRequests 1.3.6.1.2.1.2.11.15.0	read-only	Counter	The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity.
snmplnGetNexts 1.3.6.1.2.1.2.11.16.0	read-only	Counter	The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity.
snmplnSetRequests 1.3.6.1.2.1.2.11.17.0	read-only	Counter	The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity.
snmplnGetResponses 1.3.6.1.2.1.2.11.18.0	read-only	Counter	The total number of SNMP Get-Response PDUs which have been accepted and processed by the SNMP protocol entity.
snmplnTraps 1.3.6.1.2.1.2.11.19.0	read-only	Counter	The total number of SNMP Trap PDUs which have been accepted and processed by the SNMP protocol entity.
snmpOutTooBig 1.3.6.1.2.1.2.11.20.0	read-only	Counter	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is <i>tooBig</i> .
snmpOutNoSuchNames 1.3.6.1.2.1.2.11.21.0	read-only	Counter	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status is <i>noSuchName</i> .
snmpOutBadValues 1.3.6.1.2.1.2.11.22.0	read-only	Counter	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is <i>badValue</i> .

Object Name & OID	Access	Values	Description
<i>snmpOutGenErrs</i> 1.3.6.1.2.1.2.11.24.0	read-only	Counter	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is <i>genErr</i> .
<i>snmpOutGetRequests</i> 1.3.6.1.2.1.2.11.25.0	read-only	Counter	The total number of SNMP Get-Request PDUs which have been generated by the SNMP protocol entity.
<i>snmpOutGetNexts</i> 1.3.6.1.2.1.2.11.26.0	read-only	Counter	The total number of SNMP Get-Next PDUs which have been generated by the SNMP protocol entity.
<i>snmpOutSetRequests</i> 1.3.6.1.2.1.2.11.27.0	read-only	Counter	The total number of SNMP Set-Request PDUs which have been generated by the SNMP protocol entity.
<i>snmpOutGetResponses</i> 1.3.6.1.2.1.2.11.28.0	read-only	Counter	The total number of SNMP Get-Response PDUs which have been generated by the SNMP protocol entity.
<i>snmpOutTraps</i> 1.3.6.1.2.1.2.11.29.0	read-only	Counter	The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.
<i>snmpEnableAuthenTraps</i> 1.3.6.1.2.1.2.11.30.0	read-write	INTEGER <i>enabled</i> (1), <i>disabled</i> (2)	Indicates whether the SNMP agent process is permitted to generate authentication-failure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authentication-failure traps may be disabled. Note that it is strongly recommended that this object be stored in nonvolatile memory so that it remains constant between re-initializations of the network management system.

DS3/E3 MIB (RFC 1407) support

DS3 config table

Object Name & OID	Access	Values	Description
dsx3ConfigTable 1.3.6.1.2.1.10.30.5	not-accessible	SEQUENCE OF <i>Dsx3ConfigEntry</i>	The DS3/E3 Configuration table.
dsx3ConfigEntry 1.3.6.1.2.1.10.30.5.1	not-accessible	Dsx3ConfigEntry	An entry in the DS3/E3 Configuration table which consists of the following objects: <i>dsx3LineIndex</i> <i>dsx3IfIndex</i> <i>dsx3TimeElapsed</i> <i>dsx3ValidIntervals</i> <i>dsx3LineType</i> <i>dsx3LineCoding</i> <i>dsx3SendCode</i> <i>dsx3CircuitIdentifier</i> <i>dsx3LoopbackConfig</i> <i>dsx3LineStatus</i> <i>dsx3TransmitClockSource</i>
dsx3LineIndex 1.3.6.1.2.1.10.30.5.1.1.dsx 3LineIndex	read-only	INTEGER 1...65535	This object is the identifier of a DS3/E3 Interface on a managed device. If there is an <i>ifEntry</i> that is directly associated with this and only this DS3/E3 interface, it should have the same value as <i>ifIndex</i> . Otherwise, number the <i>dsx3LineIndices</i> with a unique identifier following the rules of choosing a number that is greater than <i>ifNumber</i> and numbering the inside interfaces (e.g., equipment side) with even numbers and outside interfaces (e.g., network side) with odd numbers.
dsx3IfIndex 1.3.6.1.2.1.10.30.5.1.2.dsx 3LineIndex	read-only	INTEGER 1...65535	The value for this object is equal to the value of <i>ifIndex</i> from the Interfaces table of MIB II (RFC 1213). For the IDSU, the value is 1.
dsx3TimeElapsed 1.3.6.1.2.1.10.30.5.1.3.dsx 3LineIndex	read-only	INTEGER 0...899	The number of seconds that have elapsed since the beginning of the near end current error-measurement period. The value increases monotonically with system time to 900 and then resets.
dsx3ValidIntervals 1.3.6.1.2.1.10.30.5.1.4.dsx 3LineIndex	read-only	INTEGER 0...96	The number of previous near end intervals for which valid data was collected. The value will be 96 unless the interface was brought online within the last 24 hours, in which case the value will be the number of complete 15-minute near end intervals since the interface has been online.

Object Name & OID	Access	Values	Description
dsx3LineType 1.3.6.1.2.1.10.30.5.1.5.dsx 3LineIndex	read-write	INTEGER <i>dsx3Other</i> (1), <i>dsx3M23</i> (2), <i>dsx3SYNTRAN</i> (3), <i>dsx3CbitParity</i> (4), <i>dsx3ClearChannel</i> (5), <i>e3Other</i> (6), <i>e3Framed</i> (7), <i>e3Plcp</i> (8)	This variable indicates the variety of DS3 C-bit or E3 application implementing this interface. The type of interface affects the interpretation of the usage and error statistics. The rate of DS3 is 44.736 Mbps and E3 is 34.368 Mbps. The <i>dsx3ClearChannel</i> value means that the C-bits are not used except for sending/receiving AIS. Setting these values results as follows: Set: Result: <i>dsx3Other</i> Generates an error (GenError) <i>dsx3M23</i> Sets T3 M13. <i>dsx3SYNTRAN</i> Generates an error (GenError) <i>dsx3CbitParity</i> Sets T3 C-bit. <i>dsx3ClearChannel</i> Generates an error (GenError) <i>e3Framed</i> Generates an error (GenError) <i>e3Plcp</i> Sets E3 Get will report <i>dsx3M23</i> , <i>dsx3CbitParity</i> , or <i>e3Plcp</i> for T3 M13 mode, T3 C-bit Parity Mode, or E3 Mode, respectively.
dsx3LineCoding 1.3.6.1.2.1.10.30.5.1.6.dsx 3LineIndex	read-write	INTEGER <i>dsx3Other</i> (1), <i>dsx3B3ZS</i> (2), <i>e3HDB3</i> (3)	This variable describes the variety of Zero Code Suppression used on this interface, which in turn affects a number of its characteristics. Setting these values results as follows: Set: Result: <i>dsx3Other</i> Generates an error (GenError) <i>dsx3B3ZS</i> Sets T3; generates an error for E3. <i>e3HDB3</i> Sets E3; generates an error for T3. Get will report <i>dsx3B3ZS</i> for T3 modes, <i>e3HDB3</i> for E3 mode.
dsx3SendCode 1.3.6.1.2.1.10.30.5.1.7.dsx 3LineIndex	read-write	INTEGER <i>dsx3SendNoCode</i> (1), <i>dsx3SendLineCode</i> (2), <i>dsx3SendPayloadCode</i> (3), <i>dsx3SendResetCode</i> (4), <i>dsx3SendDS1LoopCode</i> (5), <i>dsx3SendTestPattern</i> (6)	This variable indicates what type of code is being sent across the DS3/E3 interface by the device. (These are optional for E3 interfaces.) The values mean: <i>dsx3SendNoCode</i> resets any loopbacks <i>dsx3SendLineCode</i> sets remote line loopback <i>dsx3SendPayloadCode</i> sets remote payload loopback <i>dsx3SendResetCode</i> resets any loopbacks <i>dsx3SendDS1LoopCode</i> generates an error <i>dsx3SendTestPattern</i> generates an error Get normally reports <i>dsx3SendNoCode</i> .
dsx3CircuitIdentifier 1.3.6.1.2.1.10.30.5.1.8.dsx 3LineIndex	read-write	DisplayString SIZE 0...255	This variable contains the transmission vendor's circuit identifier, for the purpose of facilitating troubleshooting. Up to 20 characters. Value can be set, but is not saved in nonvolatile database.

Object Name & OID	Access	Values	Description
dsx3LoopbackConfig 1.3.6.1.2.1.10.30.5.1.9.dsx 3LineIndex	read-write	INTEGER <i>dsx3NoLoop</i> (1), <i>dsx3PayloadLoop</i> (2), <i>dsx3LineLoop</i> (3), <i>dsx3OtherLoop</i> (4)	This variable represents the loopback configuration of the DS3/E3 interface. The values mean: <i>dsx3NoLoop</i> resets any loopbacks <i>dsx3PayloadLoop</i> sets local payload loopback <i>dsx3LineLoop</i> sets local line loopback <i>dsx3OtherLoop</i> generates an error
dsx3LineStatus 1.3.6.1.2.1.10.30.5.1.10.ds x3LineIndex	read-only	INTEGER 1...1023	This variable indicates the Line Status of the interface. It contains loopback state information and failure state information. The <i>dsx3LineStatus</i> is a bit map represented as a sum, therefore, it can represent multiple failures and a loopback (see <i>dsx3LoopbackConfig</i> object for the type of loopback) simultaneously. The <i>dsx3NoAlarm</i> should be set if and only if no other flag is set. The various bit positions are: 1 <i>dsx3NoAlarm</i> No alarm present 2 <i>dsx3RcvRAIFailure</i> Receiving Yellow/Remote Alarm Indication 4 <i>dsx3XmitRAIAlarm</i> Transmitting Yellow/Remote Alarm Indication 8 <i>dsx3RcvAIS</i> Receiving AIS failure state 32 <i>dsx3LOF</i> Receiving LOF failure state 64 <i>dsx3LOS</i> Receiving LOS failure state 128 <i>dsx3LoopbackState</i> Looping the received signal <i>dsx3RcvTestCode</i> and <i>dsx3OtherFailure</i> are not returned.
dsx3TransmitClock Source 1.3.6.1.2.1.10.30.5.1.11.dsx 3LineIndex	read-write	INTEGER <i>loopTiming</i> (1), <i>localTiming</i> (2)	The source of Transmit Clock.

DS3 current table

Object Name & OID	Access	Values	Description
dsx3CurrentTable 1.3.6.1.2.1.10.30.6	not-accessible	SEQUENCE OF <i>Dsx3CurrentEntry</i>	The DS3/E3 Current table.
dsx3CurrentEntry 1.3.6.1.2.1.10.30.6.1	not-accessible	<i>Dsx3CurrentEntry</i>	An entry in the DS3/E3 Current table which consists of the following objects: <i>dsx3CurrentIndex</i> <i>dsx3CurrentPESs</i> <i>dsx3CurrentPSESs</i> <i>dsx3CurrentSEFs</i> <i>dsx3CurrentUASs</i> <i>dsx3CurrentLCVs</i> <i>dsx3CurrentPCVs</i> <i>dsx3CurrentLESs</i> <i>dsx3CurrentCCVs</i> <i>dsx3CurrentCESs</i> <i>dsx3CurrentCSESs</i>

Object Name & OID	Access	Values	Description
dsx3CurrentIndex 1.3.6.1.2.1.10.30.6.1.1.dsxC urrentIndex	read-only	INTEGER 1...65535	The index value which uniquely identifies the DS3/E3 interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value an <i>dsx3LineIndex</i> object instance.
dsx3CurrentPESs 1.3.6.1.2.1.10.30.6.1.2.dsxC urrentIndex	read-only	GAUGE	The counter associated with the number of P-bit Errored Seconds, encountered by a DS3 interface in the current 15-minute interval. The counter is incremented during AIS and OOF. The object is not valid in E3 mode.
dsx3CurrentPSEs 1.3.6.1.2.1.10.30.6.1.3.dsxC urrentIndex	read-only	GAUGE	The counter associated with the number of P-bit Severely Errored Seconds, encountered by a DS3 interface in the current 15-minute interval. The counter is incremented during AIS and OOF. The object is not valid in E3 mode.
dsx3CurrentSEFSs 1.3.6.1.2.1.10.30.6.1.4.dsxC urrentIndex	read-only	GAUGE	The counter associated with the number of Severely Errored Framing Seconds, encountered by a DS3/E3 interface in the current 15-minute interval. The counter is incremented during OOF conditions.
dsx3CurrentUASs 1.3.6.1.2.1.10.30.6.1.5.dsxC urrentIndex	read-only	GAUGE	The counter associated with the number of Unavailable Seconds, encountered by a DS3 interface in the current 15-minute interval. The counter is incremented during OOF, AIS, and Yellow alarms.
dsx3CurrentLCVs 1.3.6.1.2.1.10.30.6.1.6.dsxC urrentIndex	read-only	GAUGE	The counter associated with the number of Line Coding Violations encountered by a DS3/E3 interface in the current 15-minute interval.
dsx3CurrentPCVs 1.3.6.1.2.1.10.30.6.1.7.dsxC urrentIndex	read-only	GAUGE	The counter associated with the number of P-bit Coding Violations, encountered by a DS3 interface in the current 15-minute interval. Not valid in E3 mode.
dsx3CurrentLESs 1.3.6.1.2.1.10.30.6.1.8.dsxC urrentIndex	read-only	GAUGE	The number of Line Errored Seconds encountered by a DS3/E3 interface in the current 15-minute interval.
dsx3CurrentCCVs 1.3.6.1.2.1.10.30.6.1.9.dsxC urrentIndex	read-only	GAUGE	The number of C-bit Coding Violations encountered by a DS3 interface in the current 15-minute interval.
dsx3CurrentCESs 1.3.6.1.2.1.10.30.6.1.10.dsxC urrentIndex	read-only	GAUGE	The number of C-bit Errored Seconds encountered by a DS3 interface in the current 15-minute interval. Not valid in T3 M13 or E3 mode.
dsx3CurrentCSEs 1.3.6.1.2.1.10.30.6.1.11.dsxC urrentIndex	read-only	GAUGE	The number of C-bit Severely Errored Seconds encountered by a DS3 interface in the current 15-minute interval. Not valid in T3 M13 or E3 mode.

DS3/E3 interval table

Object Name & OID	Access	Values	Description
dsx3IntervalTable 1.3.6.1.2.1.10.30.7	not-accessible	SEQUENCE OF <i>Dsx3IntervalTableEntry</i>	The DS3/E3 Interval table.
dsx3IntervalTableEntry 1.3.6.1.2.1.10.30.7.1	not-accessible	Dsx3IntervalTableEntry	An entry in the DS3/E3 Interval table which consists of the following objects: <i>dsx3IntervalIndex</i> <i>dsx3IntervalNumber</i> <i>dsx3IntervalPESs</i> <i>dsx3IntervalPSESs</i> <i>dsx3IntervalSEFSs</i> <i>dsx3IntervalUASs</i> <i>dsx3IntervalLCVs</i> <i>dsx3IntervalPCVs</i> <i>dsx3IntervalLESs</i> <i>dsx3IntervalCCVs</i> <i>dsx3IntervalCESs</i> <i>dsx3IntervalCSESs</i>
dsx3IntervalIndex 1.3.6.1.2.1.10.30.7.1.1. <i>dsx3IntervalIndex</i>	read-only	INTEGER 1...65535	The index value which uniquely identifies the DS3/E3 interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value an <i>dsx3LineIndex</i> object instance.
dsx3IntervalNumber 1.3.6.1.2.1.10.30.7.1.2. <i>dsx3IntervalIndex</i>	read-only	INTEGER 1...96	A number between 1 and 96, where 1 is the most recently completed 15-minute interval and 96 is the least recently completed 15-minute interval (assuming that all 96 intervals are valid).
dsx3IntervalPESs 1.3.6.1.2.1.10.30.7.1.3. <i>dsx3IntervalIndex</i>	read-only	GAUGE	The counter associated with the number of P-bit Errored Seconds, encountered by a DS3 interface in one of the previous 96 15-minute intervals. Not valid in E3 mode.
dsx3IntervalPSESs 1.3.6.1.2.1.10.30.7.1.4. <i>dsx3IntervalIndex</i>	read-only	GAUGE	The counter associated with the number of P-bit Severely Errored Seconds, encountered by a DS3 interface in one of the previous 96 15-minute intervals. Not valid in E3 mode.
dsx3IntervalSEFSs 1.3.6.1.2.1.10.30.7.1.5. <i>dsx3IntervalIndex</i>	read-only	GAUGE	The counter associated with the number of Severely Errored Framing Seconds, encountered by a DS3/E3 interface in one of the previous 96 15-minute intervals.
dsx3IntervalUASs 1.3.6.1.2.1.10.30.7.1.6. <i>dsx3IntervalIndex</i>	read-only	GAUGE	The counter associated with the number of Unavailable Seconds, encountered by a DS3 interface in one of the previous 96 15-minute intervals.
dsx3IntervalLCVs 1.3.6.1.2.1.10.30.7.1.7. <i>dsx3IntervalIndex</i>	read-only	GAUGE	The counter associated with the number of Line Coding Violations encountered by a DS3/E3 interface in one of the previous 96 15-minute intervals.

Object Name & OID	Access	Values	Description
dsx3IntervalPCVs 1.3.6.1.2.1.10.30.7.1.8.dsx3IntervalIndex	read-only	GAUGE	The counter associated with the number of P-bit Coding Violations, encountered by a DS3 interface in one of the previous 96 15-minute intervals. Not valid in E3 mode.
dsx3IntervalLEsS 1.3.6.1.2.1.10.30.7.1.9.dsx3IntervalIndex	read-only	GAUGE	The number of Line Errored Seconds (BPVs or illegal zero sequences) encountered by a DS3/E3 interface in one of the previous 96 15-minute intervals.
dsx3IntervalCCVs 1.3.6.1.2.1.10.30.7.1.10.dsx3IntervalIndex	read-only	GAUGE	The number of C-bit Coding Violations encountered by a DS3 interface in one of the previous 96 15-minute intervals. Not valid in E3 mode.
dsx3IntervalCESs 1.3.6.1.2.1.10.30.7.1.11.dsx3IntervalIndex	read-only	GAUGE	The number of C-bit Errored Seconds encountered by a DS3 interface in one of the previous 96 15-minute intervals. Not valid in T3 M13 or E3 mode.
dsx3IntervalCSESs 1.3.6.1.2.1.10.30.7.1.12.dsx3IntervalIndex	read-only	GAUGE	The number of C-bit Severely Errored Seconds encountered by a DS3 interface in one of the previous 96 15-minute intervals. Not valid in T3 M13 or E3 mode.

DS3/E3 total table

Object Name & OID	Access	Values	Description
dsx3TotalTable 1.3.6.1.2.1.10.30.8	not-accessible	SEQUENCE OF <i>Dsx3TotalEntry</i>	The DS3/E3 Total table. 24-hour interval.
dsx3TotalEntry 1.3.6.1.2.1.10.30.8.1	not-accessible	<i>Dsx3TotalEntry</i>	An entry in the DS3/E3 Total table which consists of the following objects: <i>dsx3TotalIndex</i> <i>dsx3TotalPESs</i> <i>dsx3TotalPSESs</i> <i>dsx3TotalSEFSs</i> <i>dsx3TotalUASs</i> <i>dsx3TotalLCVs</i> <i>dsx3TotalPCVs</i> <i>dsx3TotalLEsS</i> <i>dsx3TotalCCVs</i> <i>dsx3TotalCESs</i> <i>dsx3TotalCSESs</i>
dsx3TotalIndex 1.3.6.1.2.1.10.30.8.1.1.dsx3TotalIndex	read-only	INTEGER 1...65535	The index value which uniquely identifies the DS3/E3 interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value an <i>dsx3LineIndex</i> object instance.

Object Name & OID	Access	Values	Description
dsx3TotalPESs 1.3.6.1.2.1.10.30.8.1.2.dsx3TotalIndex	read-only	GAUGE	The counter associated with the number of P-bit Errored Seconds, encountered by a DS3 interface in the previous 24-hour interval. Not valid in E3 mode.
dsx3TotalPSEsS 1.3.6.1.2.1.10.30.8.1.3.dsx3TotalIndex	read-only	GAUGE	The counter associated with the number of P-bit Severely Errored Seconds, encountered by a DS3 interface in the previous 24-hour interval. This object is not valid in E3 mode.
dsx3TotalSEFSs 1.3.6.1.2.1.10.30.8.1.4.dsx3TotalIndex	read-only	GAUGE	The counter associated with the number of Severely Errored Framing Seconds, encountered by a DS3/E3 interface in the previous 24-hour interval.
dsx3TotalUASs 1.3.6.1.2.1.10.30.8.1.5.dsx3TotalIndex	read-only	GAUGE	The counter associated with the number of Unavailable Seconds, encountered by a DS3 interface in the previous 24-hour interval.
dsx3TotalLCVs 1.3.6.1.2.1.10.30.8.1.6.dsx3TotalIndex	read-only	GAUGE	The counter associated with the number of Line Coding Violations encountered by a DS3/E3 interface in the previous 24-hour interval.
dsx3TotalPCVs 1.3.6.1.2.1.10.30.8.1.7.dsx3TotalIndex	read-only	GAUGE	The counter associated with the number of P-bit Coding Violations, encountered by a DS3 interface in the previous 24-hour interval. Not valid in E3 mode.
dsx3TotalLESs 1.3.6.1.2.1.10.30.8.1.8.dsx3TotalIndex	read-only	GAUGE	The number of Line Errored Seconds (BPVs or illegal zero sequences) encountered by a DS3/E3 interface in the previous 24-hour interval.
dsx3TotalCCVs 1.3.6.1.2.1.10.30.8.1.9.dsx3TotalIndex	read-only	GAUGE	The number of C-bit Coding Violations encountered by a DS3 interface in the previous 24-hour interval. Not valid in T3 M13 or E3 mode.
dsx3TotalCESs 1.3.6.1.2.1.10.30.8.1.10.dsx3TotalIndex	read-only	GAUGE	The number of C-bit Errored Seconds encountered by a DS3 interface in the previous 24-hour interval. Not valid in T3 M13 or E3 mode.
dsx3TotalCSESs 1.3.6.1.2.1.10.30.8.1.11.dsx3TotalIndex	read-only	GAUGE	The number of C-bit Severely Errored Seconds encountered by a DS3 interface in the previous 24-hour interval. Not valid in T3 M13 or E3 mode.

DS3 far-end config table

This table is not supported by the IDSU.

DS3 far-end current table

This table is only valid in T3 C-Bit Parity mode.

Object Name & OID	Access	Values	Description
dsx3FarEndCurrentTable 1.3.6.1.2.1.10.30.10	not-accessible	SEQUENCE OF <i>Dsx3FarEndCurrentTable</i>	The DS3 Far End Current table.
dsx3FarEndCurrentEntry 1.3.6.1.2.1.10.30.10.1	not-accessible	Dsx3FarEndCurrentTable	An entry in the DS3 Far End Current table which consists of the following objects: <i>dsx3FarEndCurrentIndex</i> <i>dsx3FarEndTimeElapsed</i> <i>dsx3FarEndValidIntervals</i> <i>dsx3FarEndCurrentCESSs</i> <i>dsx3FarEndCurrentCSESs</i> <i>dsx3FarEndCurrentCCVs</i> <i>dsx3FarEndCurrentUASs</i>
dsx3FarEndCurrentIndex 1.3.6.1.2.1.10.30.10.1.1.dsx3FarEndCurrentIndex	read-only	INTEGER 1...65535	The index value which uniquely identifies the DS3 interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value an <i>dsx3LineIndex</i> object instance.
dsx3FarEndTimeElapsed 1.3.6.1.2.1.10.30.10.1.2.dsx3FarEndCurrentIndex	read-only	INTEGER 0...899	The number of seconds that have elapsed since the beginning of the far end current error-measurement period.
dsx3FarEndValidIntervals 1.3.6.1.2.1.10.30.10.1.3.dsx3FarEndCurrentIndex	read-only	INTEGER 0...96	The number of previous far end intervals for which valid data was collected. The value will be 96 unless the interface was brought online within the last 24 hours, in which case the value will be the number of complete 15-minute far end intervals since the interface has been online.
dsx3FarEndCurrentCESSs 1.3.6.1.2.1.10.30.10.1.4.dsx3FarEndCurrentIndex	read-only	GAUGE	The counter associated with the number of Far End C-bit Errored Seconds encountered by a DS3 interface in the current 15-minute interval.
dsx3FarEndCurrentCSESs 1.3.6.1.2.1.10.30.10.1.5.dsx3FarEndCurrentIndex	read-only	GAUGE	The counter associated with the number of Far End C-bit Severely Errored Seconds encountered by a DS3 interface in the current 15-minute interval.
dsx3FarEndCurrentCCVs 1.3.6.1.2.1.10.30.10.1.6.dsx3FarEndCurrentIndex	read-only	GAUGE	The counter associated with the number of Far End C-bit Coding Violations reported via the far end block error count encountered by a DS3 interface in the current 15-minute interval.
dsx3FarEndCurrentUASs 1.3.6.1.2.1.10.30.10.1.7.dsx3FarEndCurrentIndex	read-only	GAUGE	The counter associated with the number of Far End unavailable seconds encountered by a DS3 interface in the current 15-minute interval.

DS3 far-end interval table

This table is only valid in T3 C-Bit Parity mode.

Object Name & OID	Access	Values	Description
dsx3FarEndIntervalTable 1.3.6.1.2.1.10.30.11	not-accessible	SEQUENCE OF <i>Dsx3FarEndIntervalEntry</i>	The DS3 Far End Interval table.
dsx3FarEndIntervalEntry 1.3.6.1.2.1.10.30.11.1	not-accessible	Dsx3FarEndIntervalEntry	An entry in the DS3 Far End Interval table which consists of the following objects: <i>dsx3FarEndIntervalIndex</i> <i>dsx3FarEndIntervalNumber</i> <i>dsx3FarEndIntervalCESs</i> <i>dsx3FarEndIntervalCSEs</i> <i>dsx3FarEndIntervalCCVs</i> <i>dsx3FarEndIntervalUASs</i>
dsx3FarEndIntervalIndex 1.3.6.1.2.1.10.30.11.1.1.dsx3FarEndIntervalIndex	read-only	INTEGER 1...65535	The index value which uniquely identifies the DS3 interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value an <i>dsx3LineIndex</i> object instance.
dsx3FarEndIntervalNumber 1.3.6.1.2.1.10.30.11.1.2.dsx3FarEndIntervalIndex	read-only	INTEGER 1...96	A number between 1 and 96, where 1 is the most recently completed 15-minute interval and 96 is the least recently completed 15-minute interval (assuming that all 96 intervals are valid).
dsx3FarEndIntervalCESs 1.3.6.1.2.1.10.30.11.1.3.dsx3FarEndIntervalIndex	read-only	GAUGE	The counter associated with the number of Far End C-bit Errored Seconds encountered by a DS3 interface in one of the previous 96 15-minute intervals.
dsx3FarEndIntervalCSEs 1.3.6.1.2.1.10.30.11.1.4.dsx3FarEndIntervalIndex	read-only	GAUGE	The counter associated with the number of Far End C-bit Severely Errored Seconds encountered by a DS3 interface in one of the previous 96 15-minute intervals.
dsx3FarEndIntervalCCVs 1.3.6.1.2.1.10.30.11.1.5.dsx3FarEndIntervalIndex	read-only	GAUGE	The counter associated with the number of Far End C-bit Coding Violations reported via the far end block error count encountered by a DS3 interface in one of the previous 96 15-minute intervals.
dsx3FarEndIntervalUASs 1.3.6.1.2.1.10.30.11.1.6.dsx3FarEndIntervalIndex	read-only	GAUGE	The counter associated with the number of Far End unavailable seconds encountered by a DS3 interface in one of the previous 96 15-minute intervals.

DS3 far-end total table

This table is only valid in T3 C-Bit Parity mode.

Object Name & OID	Access	Values	Description
dsx3FarEndTotalTable 1.3.6.1.2.1.10.30.12	not-accessible	SEQUENCE OF <i>Dsx3FarEndTotalEntry</i>	The DS3 Far End Total table. 24-hour interval.
dsx3FarEndTotalEntry 1.3.6.1.2.1.10.30.12.1	not-accessible	Dsx3FarEndTotalEntry	An entry in the DS3 Far End Total table which consists of the following objects: <i>dsx3FarEndTotalIndex</i> <i>dsx3FarEndTotalCESs</i> <i>dsx3FarEndTotalCSESSs</i> <i>dsx3FarEndTotalCCVs</i> <i>dsx3FarEndTotalUASs</i>
dsx3FarEndTotalIndex 1.3.6.1.2.1.10.30.12.1.1. dsx3FarEndTotalIndex	read-only	INTEGER 1...65535	The index value which uniquely identifies the DS3 interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value an <i>dsx3LineIndex</i> object instance.
dsx3FarEndTotalCESs 1.3.6.1.2.1.10.30.12.1.2. dsx3FarEndTotalIndex	read-only	GAUGE	The counter associated with the number of Far End C-bit Errored Seconds encountered by a DS3 interface in the previous 24-hour interval.
dsx3FarEndTotalCSESSs 1.3.6.1.2.1.10.30.12.1.3. dsx3FarEndTotalIndex	read-only	GAUGE	The counter associated with the number of Far End C-bit Severely Errored Seconds encountered by a DS3 interface in the previous 24-hour interval.
dsx3FarEndTotalCCVs 1.3.6.1.2.1.10.30.12.1.4. dsx3FarEndTotalIndex	read-only	GAUGE	The counter associated with the number of Far End C-bit Coding Violations reported via the far end block error count encountered by a DS3 interface in the previous 24-hour interval.
dsx3FarEndTotalUASs 1.3.6.1.2.1.10.30.12.1.5. dsx3FarEndTotalIndex	read-only	GAUGE	The counter associated with the number of Far End unavailable seconds encountered by a DS3 interface in the previous 24-hour interval.

DS3 fractional table

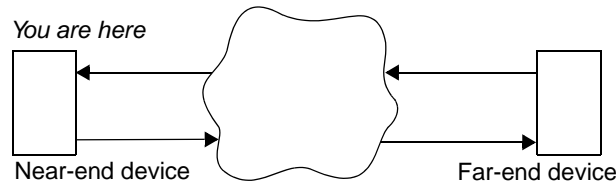
This table is not supported by the IDSU.

Glossary

AIS	Alarm Indication Signal. A signal condition and alarm indicating that the signal has been lost somewhere upstream. When a device experiences a loss of signal, it transmits an AIS signal to the next device downstream. The IDSU detects incoming AIS, but does not generate AIS.
alarm	An unsolicited message from a device that typically indicates a problem with a line.
auto-logout	A feature that automatically logs out a user if there has been no control port activity for 15 minutes.
asynchronous	Digital transmission that is not related to a specific frequency, or to timing of the transmission facility; describing transmission characterized by individual characters, or bytes, encapsulated with start and stop bits, from which a receiver derives the necessary timing for sampling bits.
bursty seconds	A second during which at least two code violations occurred, but fewer than 44 violations occurred and no out-of-frame state existed.
carrier	A company, such as any of the “baby Bell” companies, that provide network communications services, either within a local area or between local areas.
c-bit parity	A framing format derived from M13. Unlike M13, the C-bits are redefined to allow end-to-end path performance monitoring of the T3 signal and in-band data links.
CCITT	Consultative Committee for International Telephone and Telegraph. An international standards group.
code violation	<p>In the T3 M13 format, code violations are P-bit, F-bit and M-bit errors and bipolar violations (BPVs).</p> <p>In the T3 C-bit parity, code violations are the count of CP-bit, F-bit and M-bit errors and bipolar violations (BPVs).</p> <p>In the E3 format, code violations are HDB3 violations and bipolar violations (BPVs).</p>
cold-start trap	An SNMP trap that is sent when the unit has been power-cycled. <i>See also</i> trap.
control port	A port, either DTE or DCE, to which you can connect a terminal, modem, or SLIP device.

CPE	Customer Premise Equipment. Equipment that is on the customer side of the point of demarcation, as opposed to equipment that is on a carrier side. <i>See also</i> point of demarcation.
daisy chain	A string of devices that have been interconnected so that they can all be managed from one terminal.
data port	The port by which a DTE is connected to the IDSU. HSSI, V.35 and EIA-530 interface standards are supported.
DCE	Data Communications Equipment. A definition in the RS232C standard that describes the functions of the signals and the physical characteristics of an interface for a communication device such as a modem.
DSU	Data Service Unit. A DSU is a device that makes the link between a T3/E3 line and a line that is carrying packetized data streams such as those produced by a router.
DSX	Digital Signal Cross-connect.
DTE	Data Terminal Equipment. A definition in the RS232C standard that describes the functions of signals and the physical characteristics of an interface for a terminal device.
EER	Excessive Error Rate. An alarm which indicates that a threshold for the number of errored seconds or unavailable seconds has been exceeded.
EMI	Electromagnetic interference. Undesirable radiation leakage from a device that is coupled onto a transmission medium, resulting from the use of high-frequency wave energy and signal modulation. The effects can be reduced by shielding. The minimum acceptable levels are detailed by the FCC, based on the type of device and operating frequency.
EQF	Internal Equipment Failure. Something has happened to cause the internal hardware of the DataSMART T3/E3 IDSU to fail. The unit needs to be serviced.
ES	Errored Second. A measurement of the quality of the signal on a T3/E3 line defined as any second that is not an unavailable second and that contains one or more code violations.
ESD	Electro static discharge.

far-end In a relationship between two devices in a circuit, the far-end device is the one that is remote.



FEAC Far-end Alarm and Control channel. A T3 C-bit subframe used to send alarm or status information from the far-end terminal to the near-end terminal. The channel is also used to initiate T3 loopbacks at the far-end terminal from the near-end terminal.

FEBE Far-end block error functions. An FEBE C-bit parity is a parity violation detected at the far-end and transmitted back to the near-end unit.

HSSI High-speed serial interface.

IP Internet Protocol. A suite of protocols for packetizing data for shipment across LANs and WANs. Protocols exist above the IP protocol for transmitting and receiving IP packets. The DataSMART T3/E3 IDSU uses the IP protocol to provide SNMP and Telnet access.

IP address A unique 32-bit integer used to identify a device in an IP network. You will most commonly see IP addresses written in “dot” notation; for instance, 192.228.32.14. *See also* IP netmask.

IP netmask A pattern of 32 bits that is combined with an IP address to determine which bits of an IP address denote the network number and which denote the host number. Netmasks are useful for sub-dividing IP networks. IP netmasks are written in “dot” notation; for instance, 255.255.255.0. *See also* IP address.

LAN Local area network. A user-owned and -operated data transmission facility connecting numerous communication devices such as host computers, terminals, printers, and media storage units. Examples are: Ethernet, Star-LAN and Token-Ring.

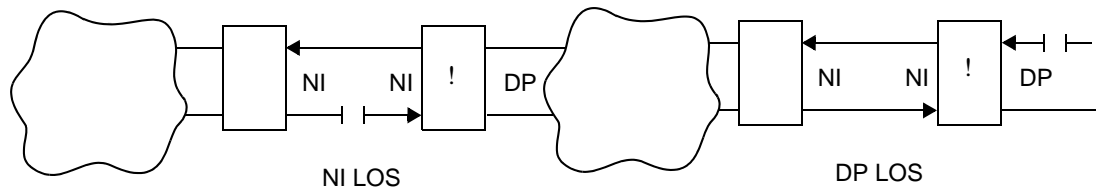
LBO Line build out. Insertion of loss in a short transmission line to make it act like a longer line.

link-down trap An SNMP trap that signifies that the T3/E3 line has transitioned from a normal state to an error state, or that a data port has been disconnected.

link-up trap An SNMP trap that signifies that the T3/E3 line, or a data port has transitioned from an error condition to a normal state.

loopback A troubleshooting technique that returns a transmitted signal to its source so that the signal can be analyzed for errors. Typically, a loopback is set at various points in a line until the section of the line that is causing the problem is discovered.

LOS Loss Of Signal. A signal condition and alarm in which the received signal at the network interface is lost.

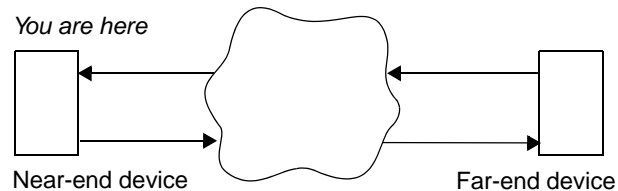


M13 An asynchronous framing format that uses all 21 T3 C-bits for bit stuffing. The standard M13 format cannot provide end-to-end path parity information.

MIB Management Information Base. The information that SNMP can access, structured as a hierarchy. In common usage of the word, MIB is in reference to a sub-branch of the entire MIB.

modem Modulator/demodulator. A device for converting a digital signal to analog (and vice versa) so that it can be transmitted over phone lines.

near-end In a relationship between two devices in a circuit, the near-end device is the one that is local.

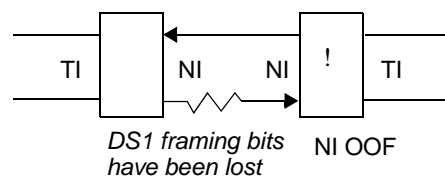


network interface (NI) Network interface. The interface between the DataSMART T3/E3 IDSU and the line supplied by the carrier.

NMS Network Management System. A tool for configuring network devices and monitoring network performance, typically an SNMP-based tool.

OID Object Identifier. The address of a MIB variable.

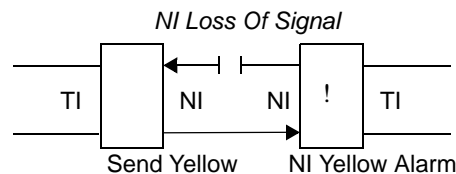
OOF Out of frame. An signal condition and alarm in which some or all framing bits are lost.



ping A protocol that is part of the TCP/IP suite, used to test the connectivity of the network. Ping sends a signal to a host or gateway, then listens for an echo response.

point of demarcation	The dividing line between a carrier and the customer premise that is governed by strict standards that define the characteristics of the equipment on each side of the demarcation. Equipment on one side of the point of demarcation is the responsibility of the customer. Equipment on the other side of the point of demarcation is the responsibility of the carrier.
PRM	Performance Report Message. Messages that are received once per second from a far-end device that report information about the condition of the far-end device.
real-time clock	A clock that maintains the time of day in distinction to a clock that is used to time the electrical pulses on a circuit.
RJ45	A type of cable connector used for RS232 lines and 10BaseT Ethernet lines.
router	A device that connects various links in a network matrix, directing packets along the most economical or efficient routes to the packet's destination; a packet switch.
RxD	Received Data. See also TxD.
SES	Severely Errored Second.
Severely Errored Framing	An SEF event is declared when three or more errors in 16 or fewer consecutive F-bits occur with a T3 M-frame.
Severely Errored Second	A second during which 44 or more code violations have occurred.
signal condition	Characteristics of the electronic pulses on a line, categorized into groups of various error types. When errored signal conditions persist they cause an alarm.
SLIP	Serial Line Interface Protocol. A protocol that allows the Internet Protocol (IP) to run on low-speed serial lines.
SMDS	Switched Multi-Megabit Digital Service. A public, high-speed, connectionless, packet-switched data transfer service that provides LAN-like performance and features over an entire metropolitan area.
SNMP	Simple Network Management Protocol. The accepted industry-standard network management protocol that uses a system of agents and managers. Each agent is responsible for interacting with a certain MIB. The manager can ask the agent for data, or it can ask the agent to set the value of some data.
super-user	A login ID that allows unlimited access to the full range of a device's functionality, especially including the ability to reconfigure the device and set passwords.
synchronous	Data communications in which characters or bits are sent at a fixed rate, with the transmitting and receiving devices synchronized; eliminates the need for start and stop bits basic to asynchronous transmission and significantly increases data throughput rates.

- T3** Communications access operating at a bit rate of 44.736 Mbps.
- TCP** Transport Control Protocol. TCP is one of the two transport protocols in the TCP/IP protocol suite. TCP is a complex, connection-based protocol that guarantees reliable delivery of packets. Telnet uses TCP.
- TCP/IP** A suite of protocols that includes IP, UDP, TCP, SNMP, TELNET, ICMP, and PING. TCP/IP is the networking protocol of choice of the Internet and many private networks as well. Kentrox SNMP and Telnet products operate in TCP/IP networks.
- Telnet** Telnet is a TCP/IP protocol that defines a client/server mechanism for emulating directly-connected terminal connections. The DataSMART T3/E3 IDSU implements a Telnet Server, allowing other devices to establish connections with it. The IDSU does not implement a Telnet Client (which would allow the IDSU to connect to other devices).
- terminal server** In the simplest terms, a terminal server is an IP network port and a collection of serial ports. Most terminal servers allow the serial ports to be configured for SLIP. If the IDSU is using SLIP, a terminal server could be used to make the connection from serial to Ethernet.
- trap** A trap is an unsolicited alert generated by SNMP. There are five standard trap types: link up, link down, warm start, cold start, and enterprise-specific. link up, link down, and cold start are supported by the IDSU.
- TxD** Transmit Data. *See also* RxD.
- UAS** Unavailable Seconds. A measurement of the signal quality of a T3/E3 line. Unavailable seconds start accruing when ten consecutive severely errored seconds occur.
- VDT** Video Display Terminal.
- warm-start trap** Warm-start traps are not supported by the IDSU.
- yellow alarm** An alarm that occurs on a device when the signal from the device is not received at the far-end.



Index

A

A bit, E3 framing, definition, 43
AC command, **33**
AC power requirements, 98
ACO status indicator, definition, 64
ACV command, **33**
ADD command, for adding trap hosts, 84
ADD command, for address screening list, 86
adding a password, 19
address screening, *see* source address screening
address, system
 viewing current value, 25
AIC, definition, 42
AIS, 65
AIS, incoming
 alarm message, 63
 enabling/disabling alarm reporting, 36
 LED indicator, 62
 status indicator, 65
 troubleshooting, 67
alarm activation criteria
 enabling/disabling EER on ES, 37
 enabling/disabling EER on UAS, 37
 enabling/disabling on incoming AIS, 36
 enabling/disabling on incoming RAI, 36
 enabling/disabling on incoming yellow, 36
Alarm Configuration menu, display, **33**, 92
alarm dial-out
 application example, 11
 enabling/disabling, 35
 entering modem string, 36
 overview, 12
 required modem settings, 35
 restrictions on use, 35
 setting control port output, 27
 string examples, 36
 viewing current modem string, 33
 viewing status via LEDs, 61
Alarm History report

 clearing data, 29, 51
 interpreting data, 58
ALARM LED, 61
alarm messages
 enabling/disabling output, 34
 monitoring, 63
 selecting control port for output, 27
 specifying ASCII or numeric, 35
 specifying output for alarm dial-out, 27
 specifying output for daisy-chained units, 27
 viewing current status, 33
alarm relay
 connecting to, *see installation guide*
 enabling/disabling, 34
 status of ACO cut-off switch, 64
 viewing current status, 33
alarms
 configuring, 32
 enabling/disabling EER on ES, 37
 enabling/disabling EER on UAS, 37
 enabling/disabling on incoming AIS, 36
 enabling/disabling on incoming RAI, 36
 enabling/disabling on incoming yellow, 36
 listing of possible alarms, 63
 setting ES threshold, 37
 setting UAS threshold, 37
 viewing current activation criteria, 34
 viewing current ES threshold, 34
 viewing current UAS threshold, 34
 viewing status via LEDs, 61
ALM status indicator, definition, 64
amplification, T3/E3 network signal, *see* transmit output level
applications, typical examples, 10
APS command, **19**
ASCII alarm format, setting, 35
attenuation, T3 network signal, *see* transmit line build-out
auto-logout, 16

B

baud rate, control port
 changing, *see installation guide*
 default setting, 31
BES (bursty errored second),
 definition, 54

C

C bits, C-Bit parity, definition, 42
C bits, M13, definition, 43
CA data port LED, 61
CA signal
 viewing status, 65
CA status indicator, definition, 65
cabling, network interface
 setting output level based on cable length, 44
 T3 transmit line build-out based on cable length, 44
C-Bit parity framing
 description of, 42
 far-end performance data, 55
 setting, 41
CC command, **31**
CCV command, **31**
character echo at control port
 enabling and disabling, 31
chassis
 back view, 9
 front view, 9
clearing data from reports, 29, 51
CLK command, **28**, 47
clock, data port
 setting receive timing, 47
 setting transmit timing, 47
clock, system, *see* source clock
code violation, definition, 54
code violations
 LED indicator, 62
 status indicator, 65
command
 DCE, 27
 DTE, 27
command-line interface
 securing with passwords, 18
 syntax, 14
 type-ahead, 14

- using menus, 13
 - commands
 - AC, 33
 - ACV, 33
 - ADD, 84, 86
 - APS, 19
 - CC, 31
 - CCV, 31
 - CLK, 28
 - DAI, 37
 - DAM, 34
 - DAR, 34
 - DDD, 35
 - DE, 31
 - DEL, 86
 - DELT, 84
 - DFP, 26
 - DIR, 35
 - DPS, 19
 - DSCRAM, 48
 - DSLIP, 79
 - DSNMP, 84
 - DST, 69
 - DSUCLK, 48
 - DYL, 36
 - EAI, 37
 - EAM, 34
 - EE, 31
 - EFP, 26
 - EIA-530, 48
 - EMS, 36
 - EPS, 21
 - ESCRAM, 48
 - ESLIP, 79
 - ESM, 35
 - ESNMP, 84
 - EST, 37
 - EUM, 35
 - EYL, 36
 - FELR, 55
 - FESR, 55
 - HSSI, 48
 - IPR, 80
 - LBO, 44
 - LM, 74
 - NC, 40
 - NCBT, 41
 - NCV, 40
 - NHI, 44
 - NLO, 44
 - NM13, 41
 - NSR, 57
 - PC, 19
 - PCV, 20
 - PE, 21
 - PEV, 22
 - PL, 50
 - R, 50
 - RCS, 83
 - RSD, 30
 - SC, 24
 - SCREEN, 85
 - SCREENV, 85
 - SCV, 24
 - SD, 26
 - SDLR, 56
 - SDT, 74
 - SLADDR, 79
 - SLL, 74
 - SLMASK, 79
 - SLO, 74
 - SN, 26
 - SNMP, 81
 - SNMPV, 81
 - SPL, 74
 - SS, 64
 - SSA, 86
 - ST, 26
 - TCP, 78
 - TCPV, 78
 - TPW, 80
 - UNLR, 53
 - UNSR, 52
 - UST, 37
 - V.35, 48
 - WCS, 83
 - WYV, 29
 - ZALL, 29
 - commands, EAR, 34
 - community strings, SNMP
 - setting, 83
 - viewing current values, 81
 - configuration password privileges, 18
 - configuring
 - alarm parameters, 32
 - control port parameters, 31
 - data port (HSSI, V.35, EIA-530), 45
 - passwords, 18
 - SLIP interface, 78
 - SNMP, 81
 - system parameters, 23
 - T3/E3 network interface, 40
 - TCP/IP, 78
 - control port
 - changing baud, parity, stop or data bits, *see installation guide*
 - changing character echo, 31
 - connector types, 99
 - factory defaults, 31
 - pin assignments, 100
 - selecting DCE or DTE for alarm output, 27
 - selecting DCE or DTE for SLIP interface, 27
 - specifications, 99
 - viewing current settings, 25
 - Control Port Configuration menu, display, **31**, 92
 - conventions, syntax, used in manual, 8
 - counters, zeroing, 29
 - CP, definition, 42
 - CTS/DCD
 - viewing status, 65
 - CTS/DCD status indicator, definition, 65
 - CV network LED, 62
 - CV status indicator, definition, 65
- ## D
- DAI command, **37**
 - daisy-chained unit
 - logging in, 15
 - DAM command, **34**, 58, 77, 79
 - DAR command, **34**
 - data bits, control port
 - changing, *see installation guide*
 - default setting, 31
 - DATA network LED, 62
 - data port
 - configuring, 45
 - monitoring transmit/receive activity via LEDs, 61
 - setting physical link type, 48
 - status display, 64
 - traffic shaping, 47
 - viewing current settings, 25, 46
 - data port, *see also* HSSI, V.35, or EIA-530
 - DATA status indicator, definition, 65
 - data terminal loopback
 - description, 73
 - resetting locally, 74
 - setting locally, 74
 - date and time
 - setting, 25
 - viewing current setting, 24

DC power requirements, 98

DCD/CTS
 viewing status, 65

DCD/CTS status indicator, definition, 65

DCE command, **27**, 77, 79

DCE control port
 selecting for alarm output, 27
 selecting for SLIP interface, 27

DDD command, **35**

DE command, **31**

default router
 specifying address, 80
 viewing current setting, 79

defaults, resetting to
 via command line, 30
 via thumbwheel switch, 30

DEL command, **86**

deleting a password, 19

DELT command, **84**

device name
 specifying new value, 26
 viewing current value, 25
 where it appears, 26

DFP command, **26**, 30

dial-out, *see* alarm dial-out

DIR command, **35**

DL, definition, 42

DP SYNC alarm
 definition, 63
 troubleshooting, 68

DPS command, **19**

DS3 config table, DS3/E3 MIB, 120

DS3 current table, DS3/E3 MIB, 122

DS3 far-end config table, DS3/E3 MIB, 126

DS3 far-end current table, DS3/E3 MIB, 127

DS3 far-end interval table, DS3/E3 MIB, 128

DS3 far-end total table, DS3/E3 MIB, 129

DS3 fractional table, DS3/E3 MIB, 129

DS3/E3 interval table, DS3/E3 MIB, 124

DS3/E3 MIB listing, 120

DS3/E3 total table, DS3/E3 MIB, 125

DSCRAM command, **48**

DSLIP command, **79**

DSNMP command, **84**

DST command, **69**

DSUCLK command, **48**

dsx3CircuitIdentifier, 121

dsx3ConfigEntry, 120

dsx3ConfigTable, 120

dsx3CurrentCCVs, 123

dsx3CurrentCESs, 123

dsx3CurrentCSESs, 123

dsx3CurrentEntry, 122

dsx3CurrentIndex, 123

dsx3CurrentLCVs, 123

dsx3CurrentLESs, 123

dsx3CurrentPCVs, 123

dsx3CurrentPESs, 123

dsx3CurrentPSESs, 123

dsx3CurrentSEFSs, 123

dsx3CurrentTable, 122

dsx3CurrentUASs, 123

dsx3FarEndCurrentCCVs, 127

dsx3FarEndCurrentCESs, 127

dsx3FarEndCurrentCSESs, 127

dsx3FarEndCurrentEntry, 127

dsx3FarEndCurrentIndex, 127

dsx3FarEndCurrentTable, 127

dsx3FarEndCurrentUASs, 127

dsx3FarEndIntervalCCVs, 128

dsx3FarEndIntervalCESs, 128

dsx3FarEndIntervalCSESs, 128

dsx3FarEndIntervalEntry, 128

dsx3FarEndIntervalIndex, 128

dsx3FarEndIntervalNumber, 128

dsx3FarEndIntervalTable, 128

dsx3FarEndIntervalUASs, 128

dsx3FarEndTimeElapsed, 127

dsx3FarEndTotalCCVs, 129

dsx3FarEndTotalCESs, 129

dsx3FarEndTotalCSESs, 129

dsx3FarEndTotalEntry, 129

dsx3FarEndTotalIndex, 129

dsx3FarEndTotalTable, 129

dsx3FarEndTotalUASs, 129

dsx3FarEndValidIntervals, 127

dsx3IfIndex, 120

dsx3IntervalCCVs, 125

dsx3IntervalCESs, 125

dsx3IntervalCSESs, 125

dsx3IntervalIndex, 124

dsx3IntervalLCVs, 124

dsx3IntervalLESs, 125

dsx3IntervalNumber, 124

dsx3IntervalPCVs, 125

dsx3IntervalPESs, 124

dsx3IntervalPSESs, 124

dsx3IntervalSEFSs, 124

dsx3IntervalTable, 124

dsx3IntervalTableEntry, 124

dsx3IntervalUASs, 124

dsx3LineCoding, 121

dsx3LineIndex, 120

dsx3LineStatus, 122

dsx3LineType, 121

dsx3LoopbackConfig, 122

dsx3SendCode, 121

dsx3TimeElapsed, 120

dsx3TotalCCVs, 126

dsx3TotalCESs, 126

dsx3TotalCSESs, 126

dsx3TotalEntry, 125

dsx3TotalIndex, 125

dsx3TotalLCVs, 126

dsx3TotalLESs, 126

dsx3TotalPCVs, 126

dsx3TotalPESs, 126

dsx3TotalPSESs, 126

dsx3TotalSEFSs, 126

dsx3TotalTable, 125

dsx3TotalUASs, 126

dsx3TransmitClockSource, 122

dsx3ValidIntervals, 120

DTE command, **27**, 35, 77, 79

DTE control port
 selecting for alarm output, 27
 selecting for SLIP interface, 27

DTR signal
 viewing status, 65

DTR status indicator, definition, 65

DYL command, **36**

E

E3 framing
 description of, 43
 setting, 41

E3 framing block, definition, 43

E3 network interface
 connector types, 99
 electrical specifications, 99
 framing, description of, 43
 monitoring performance, 49–58
 monitoring status via LEDs, 62
 monitoring transmit/receive via test jacks, 70
 setting framing format, 41
 setting transmit output level, 44
 status display, 64
 viewing current settings, 40

- EAI command, **37**
- EAM command, **34, 35**
- EAR command, **34**
- EE command, **31**
- EER alarms
 - enabling/disabling on ES, **37**
 - enabling/disabling on UAS, **37**
- EER status indicator, definition, **65**
- EFP command, **26**
- EIA-449, using as data port interface, **48**
- EIA-530 command, **48**
- EIA-530 data port
 - enabling/disabling payload scrambling, **48**
 - enabling physical link, **48**
 - monitoring transmit/receive activity via LEDs, **61**
 - pin assignments, **101**
 - setting receive timing, **47**
 - setting transmit timing, **47**
 - traffic shaping, **47**
 - viewing current settings, **46**
- EIA-530 status display, **64**
- EMS command, **35, 36**
- entering a password, **21**
- environmental specifications, **98**
- EPS command, **21**
- EQF alarm
 - definition, **63**
 - troubleshooting, **66**
- equipment failure
 - alarm message, **63**
 - troubleshooting, **66**
- errored events, definition, **37**
- error-free second, definition, **57**
- ES (errored second)
 - definition, **54**
 - use in alarm activation, **37**
- ESCRAM command, **48, 67**
- ESLIP command, **79**
- ESM command, **35, 58**
- ESNMP command, **84**
- EST command, **37**
- EUM command, **35, 58**
- excessive error rate
 - alarm message, **63**
 - troubleshooting, **68**
- external alarm, triggering, **34**
- EYL command, **36**

F

- F bits, C-Bit parity, definition, **42**
- F bits, M13, definition, **43**
- Far-end Performance report
 - clearing data, **29, 51**
 - interpreting data, **55**
 - status indicator meanings, **54**
- Far-end Short Performance Report,
 - display, **55**
- FAS, definition, **43**
- FCS errors, HDLC frames, definition, **56**
- FEAC, definition, **42**
- FEBE, definition, **42**
- FEL status indicator, definition, **64**
- FELR command, **55**
- FESR command, **55**
- fiber-optic multiplexing equipment,
 - reducing pattern sensitivity, **48**
- framing format specification
 - E3, **99**
- framing format specifications
 - T3, **98**
- framing format, T3/E3 network
 - setting, **41**
 - viewing current setting, **40**
- front-panel switch, *see* thumbwheel switch
- front-panel test jacks, **70**

H

- HDLC frames
 - FCS errors, definition, **56**
 - header errors, definition, **56**
 - length errors, definition, **56**
 - performance data, **56**
- header errors, HDLC frames,
 - definition, **56**
- HSSI command, **48**
- HSSI data port
 - enabling physical link, **48**
 - enabling/disabling payload scrambling, **48**
 - monitoring transmit/receive activity via LEDs, **61**
 - pin assignments, **100**
 - setting receive timing, **47**
 - setting transmit timing, **47**
 - specifications, **100**
 - status display, **64**
 - traffic shaping, **47**

- viewing current settings, **46**

I

- ICMP group, MIB II, **112**
- icmpInAddrMaskReps, **113**
- icmpInAddrMasks, **113**
- icmpInDestUnreachs, **112**
- icmpInEchoReps, **113**
- icmpInEchos, **113**
- icmpInErrors, **112**
- icmpInMsgs, **112**
- icmpInParmProbs, **112**
- icmpInRedirects, **113**
- icmpInSrcQuenchs, **112**
- icmpInTimeExcds, **112**
- icmpInTimestampReps, **113**
- icmpInTimestamps, **113**
- icmpOutAddrMaskReps, **114**
- icmpOutAddrMasks, **114**
- icmpOutDestUnreachs, **113**
- icmpOutEchoReps, **113**
- icmpOutEchos, **113**
- icmpOutErrors, **113**
- icmpOutMsgs, **113**
- icmpOutParmProbs, **113**
- icmpOutRedirects, **113**
- icmpOutSrcQuenchs, **113**
- icmpOutTimeExcds, **113**
- icmpOutTimestampReps, **114**
- icmpOutTimestamps, **114**
- ifAdminStatus, **106**
- ifDescr, **105**
- ifEntry, **105**
- ifIndex, **105**
- ifInDiscards, **106**
- ifInErrors, **106**
- ifInNUcastPkts, **106**
- ifInOctets, **106**
- ifInUcastPkts, **106**
- ifInUnknownProtos, **106**
- ifLastChange, **106**
- ifMtu, **106**
- ifNumber, **105**
- ifOperStatus, **106**
- ifOutDiscards, **107**
- ifOutErrors, **107**
- ifOutNUcastPkts, **107**
- ifOutOctets, **107**
- ifOutQLen, **107**
- ifOutUcastPkts, **107**
- ifPhysAddress, **106**
- ifSpecific, **107**

- ifSpeed, 106
- ifTable, 105
- ifType, 105
- input jitter tolerance
 - E3, 99
 - T3, 98
- input signal specifications
 - E3, 99
 - T3, 98
- interfaces group, MIB II, 105
- interpreting normal/abnormal
 - conditions using LEDs, 60
- IP address
 - overview, 79
 - setting new value, 79
 - viewing current address, 78
- IP address screening, *see* source
 - address screening
- IP group, MIB II, 107
- IP packets, screening, 85
- ipAddrEntry, 109
- ipAddrTable, 109
- ipAdEntAddr, 109
- ipAdEntBcastAddr, 109
- ipAdEntIfIndex, 109
- ipAdEntNetMask, 109
- ipAdEntReasmMaxSize, 109
- ipDefaultTTL, 107
- ipForwarding, 107
- ipForwDatagrams, 108
- ipFragCreates, 109
- ipFragFails, 109
- ipFragOKs, 109
- ipInAddrErrors, 108
- ipInDelivers, 108
- ipInDiscards, 108
- ipInHdrErrors, 107
- ipInReceives, 107
- ipInUnknownProtos, 108
- ipOutDiscards, 108
- ipOutNoRoutes, 108
- ipOutRequests, 108
- IPR command, **80**
- ipReasmFails, 109
- ipReasmOKs, 108
- ipReasmReqds, 108
- ipReasmTimeout, 108
- ipRouteAge, 111
- ipRouteDest, 110
- ipRouteEntry, 110
- ipRouteIfIndex, 110
- ipRouteInfo, 112

- ipRouteMask, 111
- ipRouteMetric1, 110
- ipRouteMetric2, 110
- ipRouteMetric3, 110
- ipRouteMetric4, 110
- ipRouteMetric5, 112
- ipRouteNextHop, 111
- ipRouteProto, 111
- ipRouteTable, 110
- ipRouteType, 111
- ipRoutingDiscards, 112

J

- jitter generation specification
 - E3, 99
 - T3, 98

K

- key product features, listing of, 12

L

- LBO command, **44**

- LEDs

- AIS, 62
- ALARM, 61
- CA, 61
- CV, 62
- DATA, 62
- FEI, 61
- LOOP/FEL, 61
- LOS, 62
- NEI, 61
- OOF, 62
- POWER/FAIL, 61
- RCV, 61
- RxD, 61
- SEND, 61
- TA, 62
- TxD, 61
- XMT, 61
- YEL, 62

- LEDs, interpreting normal/abnormal
 - conditions, 60

- length errors, HDLC frames,
 - definition, 56

- line build-out, *see* transmit line build-out

- line coding requirement
 - E3, 99
 - T3, 98

- line feeds, specifying for printed

- reports, 50
- line impedance specification
 - E3, 99
 - T3, 98
- line loopback
 - description, 71
 - resetting in remote device, 75
 - resetting locally, 74
 - setting in remote device, 75
 - setting locally, 74
- line rate requirement
 - E3, 99
 - T3, 98
- line-segment testing, 71
- LLB status indicator, definition, 64
- LM command, **74**
- LOC status indicator, definition, 64
- local loopback
 - description, 72
 - resetting locally, 74
 - setting locally, 74
- Local Maintenance menu, display, **74**, 91
- logging in
 - daisy-chained unit, 15
 - stand-alone unit, 15
 - Telnet access, 15
 - with password, 21
- logging out, 16
- LOOP/FEL LED, 61
- loopbacks
 - descriptions of types, 71–73
 - setting/resetting remote loopbacks, 75
 - viewing status via LEDs, 61
 - viewing status via status display, 64
- looped timing, 28
- LOS network LED, 62
- LOS status indicator, definition, 65
- loss of signal
 - alarm message, 63
 - LED indicator, 62
 - status indicator, 65
 - troubleshooting, 66

M

- M bits, C-Bit parity, definition, 42
- M bits, M13, definition, 43
- M13 framing
 - description of, 43
 - setting, 41
- Main menu, display, 13, 90

maintenance password privileges, 18
 master clock, *see* source clock, system
 menus
 Alarm Configuration, 33
 complete reference, 90–95
 Control Port Configuration, 31
 Local Maintenance, 74
 Main, 13
 Network Interface (NI)
 Configuration, 40
 Password Configuration, 19
 Password Entry, 21
 Remote Maintenance, 75
 Reports, 50
 SNMP Configuration, 81
 Source Address Screening, 85
 System Configuration, 24
 TCP/IP Configuration, 78
 MIB II listing, 104
 MM command, 13
 model number, finding, 29
 modem, alarm dial-out
 required settings, 35
 modem, alarm dial-out string
 entering, 36
 examples, 36
 viewing current setting, 33
 monitor jacks, front-panel, 70
 monitoring performance of T3/E3
 network, 49–58
 multi-rate bandwidth
 overview, 12
 multi-rate timing
 application example, 10
 setting at data port, 47
 MultiSMART manager, alarm format,
 35

N

N bit, E3 framing, definition, 43
 name, system, *see* device name
 NC command, **40**
 NCBT command, **41**
 NCV command, **40**
 Network (NI) Configuration menu,
 display, 93
 network interface
 clearing data from reports, 51
 monitoring performance, 49
 monitoring status via LEDs, 62
 monitoring transmit/receive via test
 jacks, 70

see also T3 or E3
 status display, 64
 Network Interface (NI) Configuration
 menu, display, **40**
 NHI command, **44**
 NI AIS alarm
 definition, 63
 troubleshooting, 67
 NI EER alarm
 definition, 63
 troubleshooting, 68
 NI LOS alarm
 definition, 63
 troubleshooting, 66
 NI OOF alarm
 definition, 63
 troubleshooting, 67
 NI YEL alarm
 definition, 63
 troubleshooting, 67
 NLO command, **44**
 NM13 command, **41**
 nonvolatile memory, 12
 Nr, definition, 42
 NSR command, **57**
 numeric alarm format, setting, 35

O

OOF network LED, 62
 OOF status indicator, definition, 65
 operational status, 64
 out-of-frame
 alarm message, 63
 LED indicator, 62
 status indicator, 65
 troubleshooting, 67
 output level specification
 E3, 99
 T3, 98
 output signal
 E3, 99
 T3, 98

P

P bits, C-Bit parity, definition, 42
 P bits, M13, definition, 43
 page length, specifying for reports, 50
 parity, control port
 changing *see installation guide*
 default setting, 31
 Password Configuration menu,

 display, **19**, 93
 Password Entry menu, display, **21**, 91
 password privileges
 assigning, 19
 configuration type, 18
 maintenance type, 18
 read-only type, 18
 super-user, 18
 viewing privileges of a specific
 password, 21
 viewing privileges of all passwords,
 20
 passwords
 adding, 19
 deleting, 19
 determining if any have been set, 22
 entering upon login, 21
 setting privilege levels, 19
 setting Telnet password, 80
 viewing current list, 20
 viewing current Telnet password, 78
 pattern sensitivity, reducing with
 payload scrambling, 48
 payload loopback
 description, 71
 resetting in remote device, 75
 resetting locally, 74
 setting in remote device, 75
 setting locally, 74
 payload scrambling, data port
 enabling/disabling, 48
 use in troubleshooting, 67
 viewing current setting, 25
 viewing current status, 46
 PC command, **19**
 PCV command, **20**
 PE command, **21**
 performance monitoring, T3/E3
 network, 49–58
 performance reports
 clearing data, 51
 Far-end Short Performance Report,
 display, 55
 formatting for printer, 50
 formatting for screen, 50
 HDLC performance data, 56
 status indicator meanings, 54
 Substrate Data Performance Report,
 display, 56
 User NI Long Performance report,
 display, 53
 User NI Short Performance Report,

52
 User NI Statistical Performance
 report, display, 57
 Performance Reports menu, display,
 13, **50**, 91
 PEV command, **22**
 physical link, data port, specifying, 48
 pinouts
 control port, 100
 EIA-530 data port, 101
 HSSI data port, 100
 V.35 data port, 102
 PL command, **50**
 PLB status indicator, definition, 64
 port, control, *see* control portport, data,
see data port
 power requirements, 98
 POWER/FAIL LED, 61
 PRMs, use in far-end performance
 reports, 55

R

R command, 13, **50**
 RAI, incoming
 alarm message, 63
 enabling/disabling alarm reporting,
 36
 LED indicator, 62
 status indicator, 65
 troubleshooting, 67
 RCS command, **83**
 read community string
 setting, 83
 viewing current string, 81
 read-only password privileges, 18
 receive clock, data port
 setting, 47
 reference, menus, 89
 Remote Maintenance menu, display,
75, 92
 reports
 Alarm History report, 58
 clearing data, 29, 51
 formatting for printer, 50
 formatting for screen, 50
 performance reports, 49–58
see also performance reports
 System Status, 64
 Reports menu, **50**
 Reports menu, display, 13, **50**, 91
 reset to defaults
 via command line, 30

via thumbwheel switch, 30
 restricting access to commands, 18
 RFC 1213 listing, 104
 RFC 1407 listing, 120
 RS449, using as data port interface, 48
 RSD command, 19, **30**, 51, 58
 RxD data port LED, 61

S

SC command, **24**, 45
 scalable bandwidth, *see* multi-rate
 timing
 scrambling, data port, *see* payload
 scrambling
 SCREEN command, **85**
 screening incoming IP packets, 85
 SCREENV command, **85**
 SCV command, **24**, 46
 SD command, **26**, 51, 58
 SDLR command, **56**
 SDT command, **74**
 securing the command-line interface,
 18
 security, establishing with passwords,
 18
 self-test
 LED patterns, 69
 self-test diagnostics, initiating, 69
 self-test failures
 interpreting, 61, 69
 SEND LED, 61
 serial number, finding, 29
 SES (severely errored second),
 definition, 54
 shaping traffic, data port, 47
 SLADDR command, **79**
 SLIP interface
 configuring, 78
 enabling/disabling, 79
 specifying control port, 27
 viewing current settings, 78
 SLL command, **74**
 SLMASK command, **79**
 SLO command, **74**
 SN command, **26**, 104
 SNMP
 adding/deleting hosts from address
 screening list, 86
 adding/deleting hosts from trap
 destination list, 84
 enabling/disabling agent, 84
 setting read community string, 83

setting trap community string, 83
 setting write community string, 83
 source address screening, 85
 viewing current settings, 81
 SNMP command, **81**
 SNMP Configuration menu, display,
81, 95
 SNMP group, MIB II, 117
 snmpEnableAuthenTraps, 119
 snmpInASNParseErrs, 117
 snmpInBadCommunityNames, 117
 snmpInBadCommunityUses, 117
 snmpInBadValues, 118
 snmpInBadVersions, 117
 snmpInGenErrs, 118
 snmpInGetNexts, 118
 snmpInGetRequests, 118
 snmpInGetResponses, 118
 snmpInNoSuchNames, 118
 snmpInPkts, 117
 snmpInReadOnlys, 118
 snmpInSetRequests, 118
 snmpInTooBig, 117
 snmpInTotalReqVars, 118
 snmpInTotalSetVars, 118
 snmpInTraps, 118
 snmpOutBadValues, 118
 snmpOutGenErrs, 119
 snmpOutGetRequests, 119
 snmpOutGetResponses, 119
 snmpOutNoSuchNames, 118
 snmpOutPkts, 117
 snmpOutTooBig, 118
 snmpOutTraps, 119
 SNMPV command, **81**
 source address screening
 adding/deleting hosts, 86
 enabling/disabling, 86
 Source Address Screening menu,
 display, **85**, 95
 source clock, system
 example, span not timed by carrier,
 28
 example, span timed by carrier, 28
 looping network receive signal, 28
 using internal oscillator, 28
 viewing current setting, 25
 specifications
 control port, 99
 E3 network interface, 99
 environmental, 98
 HSSI data port, 100

- T3 network interface, 98
 - V.35/EIA-530 data port, 101
- SPL command, **74**
- SS command, 63, **64**
- SSA command, **86**
- ST command, **26**, 51, 58
- stand-alone unit
 - logging in, 15
- status *see* system status, 64
- stop bits, control port
 - changing, *see installation guide*
 - default setting, 31
- subnet mask
 - setting new value, 79
 - viewing current mask value, 78
- Subrate Data Performance Report,
 - display, 56
- super-user, establishing, 18
- syntax conventions used in manual, 8
- syntax, command-line interface, 14
- sysContact, 104
- sysDescr, 104
- sysLocation, 104
- sysName, 104
- sysObjectID, 104
- sysServices, 104
- System Configuration menu, display,
 - 24**, 45, 94
- system group, MIB II, 104
- System menu, display, 90
- system parameters
 - configuring, 23
 - viewing current configuration, 24
- System Status report, display, 64
- system status, examining, 64
- sysUpTime, 104

T

- T3 framing block, definition, 42
- T3 network interface
 - C-Bit parity framing, 42
 - connector types, 98
 - electrical specifications, 98
 - M13 framing, 43
 - monitoring performance, 49–58
 - monitoring status via LEDs, 62
 - monitoring transmit/receive via test
 - jacks, 70
 - setting framing format, 41
 - setting transmit line build-out, 44
 - setting transmit output level, 44
 - status display, 64

- viewing current settings, 40
- T3 subframe, definition, 42
- TA data port LED, 62
- TA signal
 - viewing status, 62, 65
- TA status indicator, definition, 65
- TCP command, **78**
- TCP connection table, MIB II, 115
- TCP group, MIB II, 114
- TCP objects, MIB II, 116
- TCP/IP
 - viewing current settings, 78
- TCP/IP Configuration menu, display,
 - 78, 94
- tcpActiveOpens, 114
- tcpAttemptFails, 114
- tcpConnEntry, 115
- tcpConnLocalAddress, 115
- tcpConnLocalPort, 116
- tcpConnRemAddress, 116
- tcpConnRemPort, 116
- tcpConnState, 115
- tcpConnTable, 115
- tcpCurrEstab, 114
- tcpEstabResets, 114
- tcpInErrs, 116
- tcpInSegs, 115
- tcpMaxConn, 114
- tcpOutRsts, 116
- tcpOutSegs, 115
- tcpPassiveOpens, 114
- tcpRetransSegs, 115
- tcpRtoAlgorithm, 114
- tcpRtoMax, 114
- tcpRtoMin, 114
- TCPV command, **78**
- Telnet
 - logging in, 15
 - setting password, 80
 - viewing current password, 78
- temperature requirements, 98
- test jacks, front-panel, 70
- testing, line segment, 71
- thresholds, alarms
 - setting ES, 37
 - setting UAS, 37
 - viewing current settings for ES,
 - UAS, 34
- thumbwheel switch
 - complete reference of use, 96
 - enabling/disabling from command
 - line, 26

- resetting loopbacks, 75
- setting remote loopbacks, 75
- using to disable SLIP, 79
- using to reset loopbacks, 74
- using to set loopbacks locally, 74
- time intervals in reports, 52
- timing, data port
 - setting receive clock, 47
 - setting transmit clock, 47
 - viewing current settings, 25, 46
- timing, system
 - example, span not timed by carrier,
 - 28
 - example, span timed by carrier, 28
 - looping network receive, 28
 - using internal oscillator, 28
 - viewing current source, 25
- TPW command, **80**
- traffic shaping at data port, 47
- transmit clock, data port
 - setting, 47
- transmit line build-out, T3 network
 - setting, 44
 - viewing current setting, 40
- transmit output level, T3/E3 network
 - setting, 44
 - viewing current setting, 40
- trap community string
 - setting, 83
 - viewing current string, 81
- trap destination list
 - adding hosts, 84
 - deleting hosts, 84
 - viewing current values, 82
- traps
 - adding/deleting hosts to screening
 - list, 84
 - setting control port output, 27
 - types supported, 87
- triggering an external alarm, 34
- T-SMART Supervisor, alarm format,
 - 35
- TxD data port LED, 61

U

- UAS (unavailable second)
 - definition, 54
 - use in alarm activation, 37
- UDP group, MIB II, 116
- UDP listener table, MIB II, 117
- udpEntry, 117
- udpInDatagrams, 116

- udpInErrors, 116
- udpLocalAddress, 117
- udpLocalPort, 117
- udpNoPorts, 116
- udpOutDatagrams, 116
- udpTable, 117
- UNLR command, 50, **53**
- UNSR command, 50, **52**
- User NI Long Performance Report,
 - display, 53
- User NI Performance report
 - clearing data, 29, 51
 - interpreting data, 52
 - status indicator meanings, 54
- User NI Short Performance Report,
 - display, 52
- User NI Statistical report
 - clearing data, 29, 51
 - display, 57
 - interpreting data, 57
- user-interface, *see* command-line interface
- UST command, **37**

V

- V.35 command, **48**
- V.35 data port
 - enabling physical link, 48
 - enabling/disabling payload
 - scrambling, 48
 - monitoring transmit/receive activity
 - via LEDs, 61
 - pin assignments, 102
 - setting receive timing, 47
 - setting transmit timing, 47
 - specifications, 101
 - status display, 64
 - traffic shaping, 47
 - viewing current settings, 46
- version number, finding, 29
- View Address Screening, display, 85
- View Alarm Configuration, display, 33
- View Control Port Configuration,
 - display, 31
- View NI Configuration, display, 40
- View Password Configuration,
 - display, 20
- View SNMP Configuration, display, 81
- View System Configuration, 46
- View System Configuration, display, 24

- viewing current settings for
 - alarm parameters, 33
 - control port, 31
 - data port (HSSI, V.35, EIA-530), 25, 46
 - passwords, 22
 - SLIP interface, 78
 - SNMP, 81
 - system parameters, 24
 - T3/E3 network interface, 40
 - TCP/IP parameters, 78

W

- WCS command, **83**
- write community string
 - setting, 83
 - viewing current string, 81
- WYV command, **29**

X

- X bits, C-Bit Parity, definition, 42
- X bits, M13, definition, 43

Y

- YEL network LED, 62
- YEL status indicator, definition, 65
- yellow alarm, incoming
 - alarm message, 63
 - enabling/disabling alarm reporting, 36
 - LED indicator, 62
 - status indicator, 65
 - troubleshooting, 67

Z

- ZALL command, **29**, 51, 58
- zeroing counters, 29

