Lucent Technologies
Bell Labs Innovations

DSL Terminator™

Administration Guide

Part Number: 7820-0773-001
For software version 8.0
April 2000

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing, but information is subject to change.

Safety, Compliance, and Warranty Information

Before handling any Lucent Access Networks hardware product, read the *Access Networks Safety and Compliance Guide* included in your product package. See that guide also to determine how products comply with the electromagnetic interference (EMI) and network compatibility requirements of your country. See the warranty card included in your product package for the limited warranty that Lucent Technologies provides for its products.

Security Statement

In rare instances, unauthorized individuals make connections to the telecommunications network through the use of access features.

Trademarks

Copyrights for Third-Party Software Included in Lucent Access Networks Software Products

Ordering Information

You can order the most up-to-date product information and computer-based training online at http://www.lucent.com/ins/bookstore.

Feedback

Lucent Technologies appreciates your comments, either positive or negative, about this manual. Please send them to techpubs@ascend.com.

Lucent Technologies

Customer Service

Customer Service provides a variety of options for obtaining information about Lucent products and services, software upgrades, and technical assistance.

Finding information and software on the Internet

Visit the Web site at `http://www.lucent.com/ins` for technical information, product information, and descriptions of available services.

Visit the FTP site at `ftp://ftp.ascend.com` for software upgrades, release notes, and addenda.

Obtaining technical assistance

You can obtain technical assistance by telephone, email, fax, modem, or regular mail, as well as over the Internet.

Gathering information you will need

If you need to contact Lucent for help with a problem, make sure that you have the following information when you call or that you include it in your correspondence:

- Product name and model
- Software and hardware options
- Software version
- If supplied by your carrier, Service Profile Identifiers (SPIDs) associated with your line
- Your local telephone company's switch type and operating mode, such as AT&T 5ESS Custom or Northern Telecom National ISDN-1
- Whether you are routing or bridging with your Lucent product
- Type of computer you are using
- Description of the problem

Calling Lucent from within the United States

In the U.S., you can take advantage of Priority Technical Assistance or an Advantage service contract, or you can call to request assistance.

Priority Technical Assistance

If you need to talk to an engineer right away, call (900) 555-2763 to reach the Priority Call queue. The charge of $2.95 per minute does not begin to accrue until you are connected to an engineer. Average wait times are less than 3 minutes.

Advantage Services

Advantage Services is a comprehensive selection of services. Installation services help get your Lucent Wide Area Network (WAN) off to the right start. Ongoing maintenance and

support services provide hardware and software solutions to keep your network operating at peak performance. For more information, call (800) 272-3634.

Other telephone numbers

For a menu of Lucent's services, call (800) 272-3634. Or call (510) 769-6001 for an operator.

Calling Lucent from outside the United States

You can contact Lucent by telephone from outside the United States at one of the following numbers:

Telephone outside the United States	(510) 769-8027
Austria/Germany/Switzerland	(+33) 492 96 5672
Benelux	(+33) 492 96 5674
France	(+33) 492 96 5673
Italy	(+33) 492 96 5676
Japan	(+81) 3 5325 7397
Middle East/Africa	(+33) 492 96 5679
Scandinavia	(+33) 492 96 5677
Spain/Portugal	(+33) 492 96 5675
UK	(+33) 492 96 5671

For the Asia-Pacific region, you can find additional support resources at `http://www.lucent.com/ins/international/apac/`.

Obtaining assistance through correspondence

Send your technical support questions to one of the following email addresses, or correspond by fax, BBS, or regular mail with Customer Service in Lucent's U.S. offices in Alameda, CA:

- Email from within the U.S.—`support@ascend.com`
- Email from Europe, the Middle East, or Africa—`EMEAsupport@ascend.com`
- Email from the Asia-Pacific region—`apac.support@ascend.com`
- Fax—(510) 814-2312
- Customer Support BBS (by modem)—(510) 814-2302
- Write to Lucent at the following address:

  Attn: Customer Service
  Lucent Technologies
  1701 Harbor Bay Parkway
  Alameda, CA 94502-3002
  USA

Contents

Tables

About This Guide

What is in this guide

This guide contains explanations of how to administer the DSL Terminator. Following is a chapter-by-chapter description of the topics:

- Chapter 1, “System Administration,” explains how to administer and manage the DSL Terminator.
- Chapter 2, “VT100 Interface DO Commands,”describes each of the VT100 interface DO commands in alphabetic order.
- Chapter 3, “Administering Slot Cards,”explains how to view status information, remove a slot card configuration, and disable lines
- Chapter 4, “Diagnostic Commands,” lists and explains the diagnostic commands provided for WAN lines and ports.
- Chapter 5, “VT100 Interface Status Windows,” describes status windows in alphabetic order.
- Chapter 6, “Network Administration,” discusses diagnostic commands on T1and E1 lines. The chapter also discusses administering and managing TCP/IP, OSPF, multicast, Frame Relay, and X.25 networks.
- Chapter 7, “SNMP and Syslog Configuration,” explains how to configure SNMP and Syslog support.
- Appendix A, “Troubleshooting,” discusses common problems and offers possible solutions.
- Appendix B, “Diagnostic Command Reference,” lists and explains the most helpful commands available from diagnostic mode on the DSL Terminator. The chapter includes a discussion of decoding Point-to-Point (PPP) packet traces.
- Appendix C, “Upgrading System Software,” explains how to upgrade the DSL Terminator system software.

This guide also includes an index.

Note: This manual describes the full set of features for DSL Terminator units running For software version 8.0. Some features might not be available with earlier versions or specialty loads of the software.

Caution: Before installing the DSLMAX product, be sure to read safety instructions in the *Access Networks Safety and Compliance Guide*. In addition, see the *DSLMAX Hardware Installation Guide* for safety-related electrical, physical and environmental information specific to the DSLMAX unit.

What you should know

This guide is for the person who configures and maintains the DSL Terminator. To configure the unit, you need to understand Wide Area Network (WAN) concepts and Local Area Network (LAN) concepts, if applicable.

Documentation conventions

Following are all the special characters and typographical conventions used in this manual:

Convention	Meaning
`Monospace text`	Represents text that appears on your computer's screen, or that could appear on your computer's screen.
`Boldface mono-space text`	Represents characters that you enter exactly as shown (unless the characters are also in ***`italics`***—see *Italics*, below). If you could enter the characters but are not specifically instructed to, they do not appear in boldface.
Italics	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[ ]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in bold type.
|	Separates command choices that are mutually exclusive.
>	Points to the next level in the path to a parameter or menu item. The item that follows the angle bracket is one of the options that appears when you select the item that precedes the angle bracket.
Key1-Key2	Represents a combination keystroke. To enter a combination keystroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl-H means hold down the Control key and press the H key.)
Press Enter	Means press the Enter, or Return, key or its equivalent on your computer.
Note:	Introduces important additional information.
	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
	Warns that a failure to take appropriate safety precautions could result in physical injury.

Manual Set

The DSL Terminator documentation set consists of the following manuals:

- *DSL Terminator Administration Guide*
- *DSL Terminator Hardware Installation Guide*
- *DSL Terminator Configuration Guide*
- *DSL Terminator Reference*
- *TAOS RADIUS Guide*
- *TAOS Glossary*

Related publications

This guide and documentation set do not provide a detailed explanation of products, architectures, or standards developed by other companies or organizations. Here are some related publications that you may find useful:

- *The Guide to T1 Networking,* William A. Flanagan
- *Data Link Protocols,* Uyless Black
- *TCP/IP Illustrated,* W. Richard Stevens
- *Firewalls and Internet Security,* William R. Cheswick and Steven M. Bellovin

System Administration

1

Administration features

The DSL Terminator's VT100 interface provides a wide variety of features for monitoring and administering the unit's activities.The initial display of the VT100 interface shows the Main Edit Menu and a group of status windows. You configure several system administration parameters from the Main Edit Menu. The status windows display a variety of information about the operation of your DSL Terminator. You have access to DO commands, which enable you to perform additional tasks. To perform any of the administrative tasks, you must activate administrative permissions.

The VT100 interface provides access to the terminal-server command-line interface, which features a large assortment of powerful commands. For example, you can view the DSL Terminator's routing tables and statistical information. You can access detailed information about the unit's IP routing table and Frame Relay connections. You can also use the administrative commands Ping, Traceroute, and Telnet to establish and test connectivity. You can manually add, delete, or change routes in your IP routing table. Descriptions of the commands available through the terminal-server command-line interface form the major part of this chapter.

Note: You can manage the DSL Terminator from your workstation by establishing a Telnet session and logging in with sufficient administrative privileges. You can also use Telnet to manage remote DSL Terminator units.

Activating administrative permissions

Before you can use the administrative commands and profiles, you must log in as superuser by activating a Security profile that has sufficient permissions (for example, the Full Access profile.) Proceed as follows:

1 Press Ctrl-D. The DO menu appears:

```
DO...
>0=Esc
 P=Password

 C=Close TELNET

 E=Termsrv

 D=Diagnostics
```

2 Press P (or select P=Password).

3 In the list of Security profiles that opens, select Full Access.

The DSL Terminator prompts you for the Full Access password:

```
00-30p Security
Enter Password:
 []

 Press > to accept
```

4 Type the password assigned to the profile, and press Enter. The default password for the Full Access login is `Ascend.`

When you enter the correct password, the DSL Terminator displays a message informing you that the password was accepted and that the DSL Terminator is using the new security level:

```
Message #119
Password accepted.
Using new security level.
```

If the password you enter is incorrect, the DSL Terminator prompts you again for the password.

Note: The first task you should perform after logging in as the superuser is to assign a new password to the Full Access profile.

System administration parameters

Following are the VT100 system administration parameters (shown with sample settings):

```
System
   Sys Config
      Name=gateway-1
      Location=east-bay
      Contact=thf
      Date=2/20/97
      Time=10:00:29
      Term Rate=9600
      Console=Standard
      Remote Mgmt=Yes
```

```
 Max Dialout Time=20
 Parallel Dial=5
 Single Answer=Yes
 Sub-Adr=None
 Serial=0
 LAN=0
 DM=0
 Use Trunk Grps=No
 Num Trunk Digits=1
 Excl Routing=No
 Auto Logout=No
 Idle Logout=0
 DS0 Min Rst=Off
 Max DS0 Mins=N/A
 High BER=10 ** -3
 High BER Alarm=No
 No Trunk Alarm=No
 Delay Dual=No
 New NASPortID=No
 Perm Conn Update=All
 Edit=00-000
 Status 1=10-100
 Status 2=20-100
 Status 3=30-100
 Status 4=00-200
 Status 5=30-300
 Status 6=30-400
 Status 7=00-100
 Status 8=00-000
AT Answer String=
```

Understanding the administrative parameters

This section provides some background information about the administrative options. For more details about the parameters, see the DSL Terminator *Reference*. For background information about additional parameters that appear in the System profile, see the *Network Configuration Guide* for your DSL Terminator.

Name

The Name parameter specifies the system name, which can consist of up to 16 characters. Keeping the name simple (no special characters) is a good idea because it is used in negotiating bridged PPP, AIM, and BONDING connections.

Location and Contact

The Location and Contact settings are SNMP readable and settable. The Location parameter specifies the unit's location, and the Contact parameter specifies the name of the person to contact concerning any problems with the unit. You can enter up to 80 characters.

Date and Time

The Date and Time parameters set the system date and time. If you are using Simple Network Time Protocol (SNTP), the DSL Terminator can maintain its date and time by accessing the SNTP server. (For details, see the *Network Configuration Guide* for your DSL Terminator.)

Term rate and Console

The Term Rate parameter specifies the transmission rate for communications with your terminal-emulation program. Any rate higher than 9600 can cause transmission errors.

Also verify that the data rate of your terminal-emulation program is set to 9600 bps or lower.

Remote Mgmt

You can set `Remote Mgmt=Yes` to enable management of the DSL Terminator from a WAN link.

Log out parameters

The Auto Logout parameter specifies whether to log out and go back to default privileges upon loss of DTR from the serial port. Idle Logout specifies the number of minutes an administrative login can remain inactive before the DSL Terminator logs out and hangs up.

DS0 minimum and maximum resets

A DS0 minute is the online usage of a single 56-Kbps or 64-Kbps switched channel for one minute. For example, a 5-minute, 6-channel call uses 30 DS0 minutes.

The DS0 Min Rst parameter specifies when the DSL Terminator should reset accumulated DS0 minutes to 0 (zero). You can also use this parameter to specify that the DSL Terminator should disable the timer altogether.

The Max DS0 Mins parameter specifies the maximum number of DS0 minutes a call can be online. When the usage exceeds the maximum specified by the Max DS0 Mins parameter, the DSL Terminator cannot place any more calls, and it takes any existing calls offline.

High-bit-error parameters

The High BER parameter specifies the maximum bit-error rate for any PRI line. The bit-error rate consists of the number of bit errors that occur per second. The number that comes after the double asterisks specifies the power of 10 for the current ratio of error bits to total bits.

The High BER Alarm parameter specifies whether the back-panel alarm relay closes when the bit-error rate exceeds the value specified by the High BER parameter.

No Trunks Alarm

The No Trunk Alarm parameter specifies whether the back-panel alarm relay closes when all T1/PRI lines (or trunks) go out of service.

Edit and Status parameters

The Edit and Status parameters customize the status windows in the VT100 interface so that particular screens appear at startup. For details, see the *Reference* for your DSL Terminator.

Configuring the basic parameters

To configure the system name and other basic parameters in the System profile:

1 Open the System profile.

2 Specify a system name up to 16 characters long, enter the physical location of the DSL Terminator, and indicate a person to contact in case of problems. For example:

```
System
   Sys Config
      Name=gateway-1
      Location=east-bay
      Contact=thf
```

3 If necessary, set the system date and time.

```
      Date=2/20/97
      Time=10:00:29
```

4 Specify the data transfer rate of the DSL Terminator control port.

```
      Term Rate=9600
```

5 Close the System profile.

Terminal-server command-line interface

The terminal-server command-line interface provides commands for monitoring networks, initiating sessions, and administering the system.

Accessing the interface

You can start a terminal-server command-line session if you have administrative privileges. (For more information, see “Activating administrative permissions” on page 1-2). You can start a session using one of the following methods:

- From the main VT100 menu, select System > Sys Diag > Term Serv, and press Enter.
- In the Main Edit Menu, press Ctrl-D to open the DO menu, and select `E=Termsrv`.
- Enter the following keystroke sequence (Escape key, left bracket, Escape key, zero) in rapid succession:

  `Esc [ Esc 0`

If you have sufficient privileges to invoke the command line, the DSL Terminator displays a command-line prompt. For example:

```
** Ascend Terminal Server **
ascend%
```

Displaying terminal-server commands

To display the list of terminal-server commands, enter a question mark:

```
ascend% ?
```

or the Help command:

```
ascend% help
```

The system responds by listing the terminal-server commands, with brief explanations:

`?`	Displays help information
`help`	Displays help information
`quit`	Closes terminal server session
`hangup`	Closes terminal server session
`test`	test <number> frame-count.] [<optional fields>]
`local`	Go to local mode
`remote`	remote <station>
`set`	Set various items. Type ‘set ?’ for help
`show`	Show various tables. Type ‘show ?’ for help
`iproute`	Manage IP routes. Type ‘iproute ?’ for help
`telnet`	telnet [-a | -b | -t] <host-name> [<port-number>]
`ping`	ping <host-name>
`traceroute`	Trace route to host. Type 'traceroute -?' for help
`rlogin`	rlogin [-l user -ec] <host-name> [-l user]
`kill`	terminate session

Returning to the VT100 menus

The following commands close the terminal-server command-line interface and return the cursor to the VT100 menus:

```
quit            Closes terminal server session
hangup          Closes terminal server session
local           Go to local mode
```

For example:

```
ascend% quit
```

When a user enters the Local command, a Telnet session begins.

Commands for monitoring networks

The following commands are specific to IP routing connections:

```
iproute             Manage IP routes.  Type 'iproute ?' for help
ping                ping <host-name>
traceroute          Trace route to host.  Type 'traceroute -?' for help
```

For details about each of the commands, see Chapter 6, "Network Administration."

Commands for use by terminal-server users

The following commands must be enabled for use in Ethernet > Mod Config > TServ Options. If they are enabled, login users can initiate a session by invoking the commands in the terminal- server interface.

```
telnet              telnet [ -a|-b|-t ] <host-name> [ <port-number> ]
rlogin              rlogin [ -l user -ec ] <host-name> [ -l user ]
```

These commands initiate a session with a host or modem, or toggle to a different interface that displays a menu selection of Telnet hosts.

Telnet

The Telnet command initiates a login session to a remote host. It uses the following format:

where **telnet** [-a|-b|–t] ***hostname*** [***port-number***]

- **–a | –b | –t** are optional arguments specifying ASCII, Binary, or Transparent mode, respectively. If one of the arguments is entered, it overrides the setting of the Telnet Mode parameter.
  In ASCII mode, the DSL Terminator uses standard 7-bit mode. In Binary mode, the DSL Terminator tries to negotiate 8-bit mode with the server at the remote end of the connection, so that the user can send and receive binary files by means of 8-bit file transfer protocols. In transparent mode, either of the other modes can be used without specifying the node.
- **hostname** can be the remote system's DNS name if you have configured DNS. If you have not, you must specify the IP address of the remote system.
- **port-number** is an optional argument specifying the port to use for the session. The default is 23, which is the port number of the well-known port for Telnet.

For example, if your DNS table has an entry for `myhost`, you can open a telnet session with that host as follows:

```
ascend% telnet myhost
```

If you do not configure DNS, you must specify the host's IP address instead. There are also several options in the Ethernet > Mod Config > TServ Options subprofile that affect Telnet; for example, if you set Def Telnet to Yes, you can just type a hostname to open a Telnet session with that host:

```
ascend% myhost
```

Another way to open a session is to invoke Telnet first, then enter the Open command at the Telnet prompt. For example:

```
ascend% telnet
telnet> open myhost
```

When your screen displays the `telnet>` prompt, you can enter any of the Telnet commands described in "Telnet session commands" on page 1-8. You can quit the Telnet session at any time by entering the Quit command at the Telnet prompt:

```
telnet> quit
```

Note: During an open Telnet connection, press Ctrl-] to display the `telnet>` prompt and the Telnet command-line interface. Any valid Telnet command returns you to the open session. Note that Ctrl-] does not function in binary mode Telnet. If you log into the DSL Terminator by Telnet, you might want to change the escape sequence from Ctrl-] to a different setting.

Telnet session commands

The commands in this section can be entered at the Telnet prompt during an open session. To display the Telnet prompt while logged in to a host, press Ctrl-] (hold down the Control key and type a right bracket). To display information about Telnet session commands, use the Help or ? command. For example:

```
telnet> ?
```

To open a Telnet connection after invoking Telnet, use the Open command. For example:

```
telnet> open myhost
```

To send standard Telnet commands such as Are You There or Suspend Process, use the Send command. For example:

```
telnet> send susp
```

For a list of Send commands and their syntax, enter the Send command with a question mark:

```
telnet> send ?
```

To specify special characters for use during the Telnet session, use the Set command. For example:

```
telnet> set eof ^D
```

To display current settings, enter the Set All command:

```
telnet> set all
```

To display a list of Set commands, enter the Set command with a question mark:

```
telnet> set ?
```

To quit the Telnet session and close the connection, enter the Close or Quit command. For example:

```
telnet> close
```

Telnet error messages

The DSL Terminator generates an error message for any condition that causes the Telnet session to fail or terminate abnormally. The following error messages can appear:

- `no connection: host reset`—The destination host reset the connection.

- `no connection: host unreachable`—The destination host is unreachable.
- `no connection: net unreachable`—The destination network is unreachable.
- `Unit busy. Try again later.`—The host already has open the maximum number of concurrent Telnet sessions.

Rlogin command

The Rlogin command initiates a login session to a remote host. The command has the following format:

`rlogin [-`*`echar`*`] `*`hostname`*` [-1`*`username`*`]`

where:

- -e*char* sets the escape character to *char*. For example:

  ```
  rlogin -e$ 10.2.3.4
  ```

  The default escape character is a tilde (~).
- ***`hostname`*** can be the remote system's DNS name if you have configured DNS. If oyu have not, you must specify the IP address of the remote system.
- ***`-lusername`*** specifies that you log into the remote host as ***`username`***, rather than as the name with which you logged into the terminal server. (If you logged in through RADIUS or TACACS, you must be prompted for this option.) If you can specify this option on the command line, you can enter it either before or after the hostname argument. For example, the following two lines perform identical functions:

  ```
  rlogin -l jim 10.2.3.4
  rlogin 10.2.3.4 -l jim
  ```

To terminate the remote login, choose the Exit command at the remote system's prompt. Or, you can press the Enter key, then type the escape character followed by a period.

```
<CR><ESC-CHAR><PERIOD>
```

For example, to terminate a remote login that was initiated with the default escape character (a tilde), press the Enter key, then the ~ key, then the . key.

TCP

The TCP command initiates a login session to a remote host. The command has the following format:

`tcp` ***`hostname`*** [***`port-number`***]

where:

- ***`hostname`*** can be the remote system's DNS name if you have configured DNS. If oyu have not, you must specify the IP address of the remote system.
- ***`port-number`*** specifies the port to use for the session. The port number typically indicates a custom application that runs on top of the TCP session. For example, port number 23 starts a Telnet session. However, terminating the Telnet session does not terminate the raw TCP session.

When the raw TCP session starts running, the DSL Terminator displays the word `connected`. You can then use the TCP session to transport data by running an application on

top of TCP. You can hang up the device at either end to terminate the raw TCP session. If you are using a remote terminal-server session, ending the connection also terminates raw TCP.

If a raw TCP connection fails, the DSL Terminator returns one of the following error messages:

- `Cannot open session:` hostname port-number—You entered an invalid or unknown value for *`hostname`*, you entered an invalid value for *`port-number`*, or a port number was required and you failed to enter it.
- `no connection: host reset`— The destination host reset the connection.
- `no connection: host unreachable`— The destination host is unreachable.
- `no connection: net unreachable`— The destination network is unreachable.

Administrative commands

The following commands (shown as they appear in the Help display) are useful for system administration:

remote	`remote <station>`
set	`Set various items. Type 'set ?' for help`
show	`Show various tables. Type 'show ?' for help`
kill	`terminate session`

Remote

After an MP+ connection has been established with a remote station (for example, by using the DO Dial command), you can start a remote management session with that station by entering the Remote command in the following format:

`remote` ***`station`***

For example:

`ascend%` **`remote lab17gw`**

During the remote management session, the user interface of the remote device replaces your local user interface, as if you had opened a Telnet connection to the device. You can enter Ctrl-\ at any time to terminate the Remote session. Note that either end of an MP+ link can terminate the session by hanging up all channels of the connection.

The argument to the Remote command is the name of the remote station. It must match the value of a Station parameter in a Connection profile that allows outgoing MP+ calls, or the `user-id` at the start of a RADIUS profile set up for outgoing calls.

Note: A remote management session can time out because the traffic it generates does not reset the idle timer. Therefore, the Idle parameter in the Connection profile at both the calling and answering ends of the connection should be disabled during a remote management session, and restored just before exiting. Remote management works best at higher terminal speeds.

At the beginning of a remote management session, you have privileges set by the default Security profile at the remote end of the connection. To activate administrative privileges on

the remote station, activate the appropriate remote Security profile by using the DO Password command (as described in “Activating administrative permissions” on page 1-2).

The DSL Terminator generates an error message for any condition that causes the test to terminate before sending the full number of packets. The following error messages can appear:

Message	Explanation
not authorized	Your current security privileges are insufficient for beginning a remote management session. To assign yourself the required privileges, log in with the DO PASSWORD command to a Security profile whose Edit System parameter is set to Yes.
cannot find profile for <station>	The DSL Terminator could not locate a local Connection profile containing a Station parameter whose value matched <station>.
profile for <station> does not specify MPP	The local Connection profile containing a Station value equal to <station> did not contain Encaps=MPP.
cannot establish connection for <station>	The DSL Terminator located a local Connection profile containing the proper Station and Encaps settings, but it could not complete the connection to the remote station.
<station> did not negotiate MPP	The remote station did not negotiate an MP+ connection. This error occurs most often when the remote station does not support MP+, but does support PPP.
far end does not support remote management	The remote station is running a version of MP+ that does not support remote management.
management session failed	A temporary condition, such as premature termination of the connection, caused the management session to fail.
far end rejected session	The remote station was configured to reject remote management; its Remote Mgmt parameter was set to No in the System profile.

Set

The Set command takes several arguments. To display them, enter the Set command with a question mark:

```
ascend% set  ?

set ?               Display help information
set all             Display current settings
set term            Sets the telnet/rlogin terminal type
set password        Enable dynamic password serving
set fr              Frame Relay datalink control
set circuit         Frame Relay Circuit control
set sessid [val]    Set and store [val] or current id
set arp clear       Clear arp cache
set stat            Clear statistics
set sdsl            sdsl control
```

The Set All command displays current settings. For example:

```
ascend% set all
```

```
term = vt100
dynamic password serving = disabled
```

To specify a terminal type other than VT100, use the Set Term command.

The Set Password command puts the terminal server in password mode, in which a third-party ACE or SAFEWORD server at a secure site can display password challenges dynamically in the terminal-server interface. When the terminal server is in password mode, it passively waits for password challenges from a remote ACE or SAFEWORD server. The Set Password command applies only when using security card authentication. Enter the command as follows:

```
ascend% set password
Entering Password Mode...

[^C to exit] Password Mode>
```

To return to normal terminal-server operations and thereby disable password mode, press Ctrl-C.

Note that each channel of a connection to a secure site requires a separate password challenge, so for multichannel connections to a secure site, you must leave the terminal server in password mode until all channels have been established. The APP Server utility provides an alternative way to allow users to respond to dynamic password challenges obtained from hand-held security cards.

The Set FR commands enable you to bring down the nailed connection specified in the named Frame Relay profile. The connection reestablished within a few seconds. The Set Circuit commands let you activate or deactivate a Frame Relay circuit.

Show

The Show command takes several arguments. To display them, enter the Show command with a question mark:

```
ascend% show ?
```

`show ?`	Display help information
`show arp`	Display the arp cache
`show icmp`	Display ICMP information
`show if`	Display Interface info. Type 'show if ?' for help
`show ip`	Display IP information. Type 'show ip ?' for help
`show udp`	Display UDP information. Type 'show udp ?' for help
`show igmp`	Display IGMP information. Type 'show igmp ?' for help
`show mrouting`	Display MROUTING information. Type 'show mrouting ?' f ?'
`show tcp`	Display TCP information. Type 'show tcp ?' for help
`show fr`	Display Frame relay info. Type 'show fr ?' for help
`show pools`	Display the assign address pools
`show sdsl`	Display SDSL information
`show uptime`	Display system uptime
`show revision`	Display system revision
`show users`	Display concise list of active users
`show filters`	Display filters of active users. Type 'show filters <ID>'
`show sessid`	Display current and base session id

Note: Many of the Show commands are specific to a particular type of usage, such as, IP routing. The chapters of this guide that relate to these types of connection and routing describe the relevant Show commands.

Show Uptime

To see how long the DSL Terminator has been running, enter the Show Uptime command. For example:

```
ascend% show uptime
system uptime: up 2 days, 4 hours, 38 minutes, 43 seconds
```

If the DSL Terminator stays up for 1000 consecutive days with no power cycles, the number of days displayed resets to 0 and begins to increment again.

Show Revision

The Show Revision command displays the software load and version number currently running on the DSL Terminator. For example:

```
ascend% show revision
techpubs-lab-17 system revision: ebiom.m40 5.0A
```

Show Users

To display the number of active sessions, enter the Show Users command. For example:

```
ascend% show users
I Session    Line: Slot: Tx    Rx    Service    Host         User
O ID         Chan  Port  Data  Rate  Type[mpID] Address      Name
O 231849873  1:1   9:1   56K   56K   MPP[1]     10.10.68.2   jdoe
I 231849874  1:3   3:1   28800 33600 Termsrv    N/A          Modem 3:1
O 214933581  1:2   9:2   56K   56K   MPP[1]     10.10.4.9    arwp50
O 214933582  1:6   9:3   56K   56K   MPP[1]     MPP Bundle   arwp50
```

The output includes the following fields:

Field	Content
IO	I for an incoming call or O for an outgoing call
Session ID	Unique session-ID. This is the same as Acct-Session-ID in RADIUS.
Line:Chan	Line and channel on which the session is established.
Slot: Port	Slot and port of the service being used by the session. Can indicate the number of a slot containing a modem card, and the modem on that card. Or can indicate the virtual slot of the DSL Terminator's bridge/router, with the port indicator showing the virtual interfaces to bridge/router starting with 1 for the first session of a multichannel session.
Tx Data	Transmit data rate in bits per second.
Rx Rate	Receive data rate in bits per second.
Service Type	Type of session, which can be Termsrv or a protocol name. For MP and MPP (MPT), shows the bundle ID shared by the calls in a multichannel session. The special values `Initial` and `Login` document the progress of a session. `Initial` identifies sessions that do not yet have a protocol assigned. `Login` identifies Termsrv sessions during the login process.
Host Address	Network address of the host originating the session. For some sessions this field is N/A. For outgoing MPP sessions only, the first connection has a valid network address associated with it. All other connections in the bundle have the network address listed as `MPP Bundle.`
User Name	The station name associated with the session. Initially, the value is `Answer`, which is usually replaced with the name of the remote host. For terminal-server sessions User Name is the login name. Before completion of login, the field contains the string `modem x:y` where `x` and `y` are the slot and port, respectively, of the modem servicing the session.

Kill

The Kill command enables you to disconnect a user who establishes a Telnet connection to the DSL Terminator. You can disconnect the user by specifying the session ID. The resulting disconnect code is identical to the RADIUS disconnect code, allowing you to track all administrative disconnects. To terminate a Telnet session, enter the command as follows:

kill *session ID*

where ***session ID*** is the session ID as displayed by the Show Users command described in the preceding section. The reported disconnect cause is DIS_LOCAL_ADMIN. The active Security profile must have Edit All Calls set to Yes. If Edit All Calls=No, the following message appears when you enter the Kill command:

```
Insufficient security level for that operation.
```

When the session is properly terminated, a message similar to the following appears:

```
Session 216747095 killed.
```

When the session is not terminated, a caution similar to the following appears:

```
Unable to kill session 216747095.
```

VT100 Interface DO Commands

2

Using DO commands

The DO menu is a context-sensitive list of commands that appears when you press Ctrl-D. The commands in the DO menu vary, depending on the context in which you invoke it. For example, if you press Ctrl-D in a Connection profile, the DO menu looks similar to the following:

```
DO...
>0=ESC
 P=Password
 S=Save
 E=Termserv
 D=Diagnostics
```

To execute a DO command, press and release the Ctrl-D on a VT-100 system, and then press and release the next key in the sequence (such as 1 to invoke the Dial command.) On a VT100 terminal, The PF1 function key is equivalent to Ctrl-D.

Table 2-1 lists all the DO commands. The availability of a particular command depends on your location in the interface and your permission level.

Table 2-1. DO commands

Command	Description
Close TELNET (DO C)	Close the current Telnet session.
Diagnostics (DO D)	Access the diagnostic interface.
ESC (DO 0)	Abort and exit the DO menu.
Menu Save (DO M) 8	Save the VT100 interface menu layout.
Password (DO P) 9	Log into or out of the DSL Terminator.
Termmserv (DO E)	Access the terminal- server interface.

DO commands in alphabetic order

This section describes the DO commands in detail.

Close Telnet (DO C)

The DO Close Telnet command closes the current Telnet session. You must be running a Telnet session from the DSL Terminator's terminal-server interface.

Diagnostics (DO D)

The DO D command invokes diagnostics mode. The user must have sufficient privileges in the active Security profile. In diagnostics mode, the VT100 interface displays a command-line prompt:

```
>
```

Use the help ascend command to display a list of diagnostic commands:

```
> help ascend
```

To exit diagnostics mode and return to the VT100 interface, enter the Quit command:

```
> quit
```

Esc (DO 0)

The DO ESC command exits the DO menu.

Password (DO P)

The DO Password command enables you to log into the DSL Terminator. During login, you select and activate a Security profile. The Security profile remains active until you log out or replace it by activating a different Security profile, or until the DSL Terminator automatically logs you out. The DSL Terminator can have several simultaneous user sessions and, therefore, several simultaneous Security profiles.

To log into the DSL Terminator, use the DO P command. You can log in or log out from any menu. Whenever you select the DO P command, a list of Security profiles appears. Select the desired profile with the Enter or Right Arrow key, and enter its corresponding password when prompted. If you enter the correct password for the profile, the security of the DSL Terminator is reset to the Security profile you have selected.

If you select the first Security profile, Default, simply press Enter or Return when prompted for a password. The password for this profile is always null.

If you are operating the DSL Terminator locally and you want to secure the DSL Terminator against the next user, use the DO P command and select the first profile, Default. Typically, the Default profile has been edited to disable all operations you wish to secure.

The DSL Terminator logs you out to the Default profile if any one of the following situations occurs:

- You end a console session.
- You exceed the time set by the Idle Logout parameter in the System profile.

```
Auto Logout=Yes in the System profile and you are connected to
the VT100 control port.
```

A single Security profile can be used simultaneously by any number of users. If both you and another user enter the same password, you both get the same Security profile and can perform the same operations. If each of you uses a different password to log in, each of you gets a separate Security profile with separate lists of privileges.

If you edit a Security profile, the changes do not affect anyone who is logged in and using that profile. However, the next time someone logs in and uses that profile, security for the user will be limited according to the changes you have made.

For related information, see the Auto Logout and Idle Logout parameters in the DSL Terminator *Reference*.

Termserv (DO E)

The DO Termserv command invokes the terminal-server command-line interface. The user must have sufficient privileges in the active Security profile. In terminal-server mode, the VT100 interface displays a command-line prompt. By default the prompt is:

```
ascend%
```

Enter the Help command to display a list of terminal-server commands:

```
ascend% help ascend
```

For examples that use terminal-server commands, see the DSL Terminator *Reference*. To exit terminal-server mode and return to the VT100 interface, enter the Quit command:

```
ascend% quit
```

Administering Slot Cards

3

Slot card administration

The DSL Terminator has two expansion slots, which support several types of cards. Typical system administration tasks for the DSL Terminator slot cards include viewing status information, removing a slot card configuration, and disabling lines. For information about managing the DSL Terminator system, see Chapter 1, “System Administration.”

Viewing installed slot cards

The Main Edit Menu displays any slot cards installed in the DSL Terminator. The following example illustrates the display of an DSL Terminator that has DS3-ATM and UDS3 cards installed:

```
Main Edit Menu

    00-000 System
   >10-000 Net/DS3-ATM
    20-000 Net/UDS3
    30-000 Ethernet
```

This table illustrates the labels that appear in the Main Edit Menu and the type of card the label designates. ;

Label	**Designates**
Net/8E1	8-line E1 slot card
`Net/8T1`	8-line T1 slot card
`Net/DS3-ATM`	DS3 card with ATM support

Label	Designates
Net/8E1	8-line E1 slot card
Net/8T1	8-line T1 slot card
Net/OC3-SMF-ATM	OC3 card with ATM support.
Net/UDS3	Unchannelized DS3 card

Viewing information about a particular slot card

The WAN slots are slot 1 and slot 2 (menus 10-000 and 20-000). The contents of these slots differ depending on the types of cards you have installed.

Following is an example of a UDS3 menu and a DS3-ATM menu:

```
10-000 Net/UDS3
   10-100 Line Config
          any profile
             Name=
             Enabled=No
             Nailed-group=0
             TrnkGrp=0
             Line 1...
               Activation=Static
               Line Type=C-bit parity
               Line Coding=B3ZS
               Loopback=None


   10-200 Line Diag
       10-201 LoopBack
                0=ESC
              1=Set


20-000 Net/DS3-ATM
   20-100 Line Config
          any profile
             Name=
             Enabled=No
             Nailed-group=0
             TrnkGrp=0
             Line 1...
               Activation=Static
               Framer mode=C-bit PLCP
               Loopback=None
               Long Cable ( >256ft)=None
               Vpi/Vci range=0-15/32-4095
   20-200 Line Diag
         20-201 Loopback
                  0=ESC
                1=Set
```

Following is an example of OC3-ATM menu:

```
20-000 Net/OC3-ATM
   20-100 Line Config
          any profile
             Name=
             Enabled=No
             Nailed-group=0
             TrnkGrp=0
             Line 1...
               >Loopback=Local
                Framer Rate=STS-3c
                Rx Descramble Disabled=No
                Tx Scramble Disabled=No
                Rx Pyld Dscrmb Disabled=No
                Tx Pyld Scrmb Disabled=No
                Loop Timing=No
                Vpi/Vci range=0-15/32-4095
             Traffic Shapers...
               >Enabled = No
                Bit Rate=1000
                Peak Rate=1000
                Max Burst Size=2
                Aggregate=No
                Priority=0
```

Following is an example of a T1 or E1 menu:

```
   10-000 Net/8T1 (or Net/8E1)
      10-100 Line Config
         any profile
                Name=
                Line 1...
                   Enabled=Yes
                   Nailed Group=0
                   Framing Mode=ESF
                   Front End=CSU
                   Encoding=B8ZS
                   Length=N/A
                   Buildout=0 dB
                   Clock Source=Yes
                   First DS0 channel=1
                    Last DS0 channel=24
                Line 8...

      10-200 Line Diag
        10-201 Line LB1
                  0=ESC
                  1=Line 01 LB
        ...
        ...
        ...
        10-208 Line LB8
```

Administering DS3-ATM cards

Important information about DS3 card operation can be obtained from the status window. A number of diagnostic commands are available to assist in troublshooting DS3 problems.

Interpreting status windows for the DS3 card

Use status profiles on the VT100 interface to perform diagnositcs on the DS3-ATM card. you can view available lines, each line's status, and any error on each line. The DSL Terminator displays available lines in the Main Edit Menu:

```
Main Edit Menu
00-000 System
10-000 Net/DS3-ATM
20-000 Net/DS3-ATM
30-000 Ethernet
```

The DSL Terminator dislays the status of the available lines in the Line Status profile:

```
10-000 Net/DS3-ATM
10-100 Line Status
10-200 Line Errors
```

When you select Line Status, the DSL Terminator displays the current status of that Net/DS3-ATM line. An asterik (**`*`**) character in any column indicates that the state applies. A hyphen (**`-`**) character in any column indicates that the state does not apply. The following table describes the possible states for Net/DS3-ATM Line Status:

State	Description
ACT	On indicates multipoint established.
OOF	On indicates the near end is in an out-of-frame condition.
RED	On indicates the line is not connected, improperly configured, experiencing a very high error rate, or supplying inadequate synchronization.
YEL	On indicates the card is receiving a yellow-alarm from far end.
AIS	On indicates the card is receiving an alarm indication signal.

Example:

```
10-000 DS3-ATM
ACT OOF RED YEL AIS
*   -   -   -   -
```

Using diagnostic commands

The DO menu is a context-sensitive list of commands that appears when you press Ctrl-D. The commands in the DO menu vary, depending on the context in which you invoke it. For example, if you press Ctrl-D in a Connection profile, the DO menu looks similar to the following:

```
DO...
>0=ESC
 1=Dial
 P=Password
 S=Save
 E=Termserv
 D=Diagnostics
```

To execute a DO command, press and release the Ctrl-D on a VT100 system, and then press and release the next key in the sequence (such as 1 to invoke the Dial command.) On a VT100 terminal, the PF1 function key is equivalent to Ctrl-D.

In Diagnostics, you may use the following supported command:

```
> atmframer slot-[t|d|l|r|s|c]
```

Here are the options and effects for each of the atmframer slot commands:

Option	Effect
`-t`	Toggles debug output.
`-d`	Dump ATM framer chip status information. The information this option displays is also available from the status lights on the card and in the DS3-ATM-Stat profile.
`-l`	Toggle a local loopback.
`-r`	Toggle a remote loopback.
`-s`	Synchronize to the DS3-ATM profile. The DSL Terminator automatically rereads the line configuration whenever it comes up.
`-c`	Clear the error counters.
`-?`	Displays this summary.

For example, to view overall status information about the DS3-ATM line, enter the framer command with the `-d` option:

```
> atmframer slot-d
Framer is Enabled

RED_ALARM_LED   : Off
YELLOW_ALARM_LED: Off
AIS_LED         : Off
OOF_LED         : Off
ACTIVE_LED      : On


F-Bit  Error Counter: 35
P-Bit  Error Counter: 20
C-PBit Error Counter: 10
```

```
FEB    Error Counter: 51
BPV    Error Counter: 12
EZD    Error Counter: 39
```

The following parameters indicate the errors on the DS3 line. (Refer to RFC 1407 for complete description of these errors.)

Parameter	Description
F Bit Error Counter	Framing bit errors received since the last DSL Terminator reset or the error counters were cleared.
P Bit Error Counter	P-bit errors indicate that DSL Terminator received a P-bit code on the DS3 M-frame that differs from the locally calculated code.
CP Bit Error Counter	For C-Bit-Parity lines indicates the number of parity errors since the last DSL Terminator reset.
FEB Error Counter	Far-end block errors received since the last DSL Terminator reset.
BPV Error Count	Bipolar Violation (BPV) errors may indicate that the line sent consecutive one bits with the same polarity. It could also mean that three or more consecutive zeroes were sent or an incorrect polarity.
EZD Error Counter	Number of Excessive Zero Detect (EZD) line code violations that have occurred since the error counters were cleared.

The ATMDumpCall command is a low-level management tool for use during diagnostic sessions with the DS3-ATM card.

> `atmdumpcall -`*`option`*

where *`-option`* is one of the following:

Option	Effect
`-a`	Display all ATM call blocks, even those that are inactive.
-l	Display DS3-ATM line configuration information.
`-u`	Display in-use ATM call blocks.

For example, to view all ATM call blocks, enter the ATMDumpCall command with the `-a` option:

```
> atmdumpcall -a
atmdumpcall -a
ATM Call Block Table:
Addr.     Index Active  callID  routeID State     Vpi/Vci     Prof_Name  Sess_Up
E00C47F0  0     1       1       1       CONNECTED 1/43        atm-30-sw  Yes
E00C4834  1     1       2       2       CONNECTED 15/1023     Yossi-TNT  Yes
E00C4878  2     1       3       3       CONNECTED 1/56        Yoss-P220  Yes
E00C48BC  3     0       65535   0       INACTIVE  0/0           -        No
E00C4900  4     0       65535   0       INACTIVE  0/0           -        No
```

```
.
.
.
E00C5868  62    0       65535   0       INACTIVE  0/0           -        No
E00C58AC  63    0       65535   0       INACTIVE  0/0           -        No

ATM Free Blocks: 360
ATM Used Blocks: 0
```

Looping back the DS3-ATM line

For diagnostics, you might want to loopback the DS3 interface by using the Loopback parameter in the DS3-ATM profile. While the interface is looped back, normal data traffic is interrupted. The Loopback parameter in the DS3-ATM profile supports the following settings:

Value	Description
No-Loopback	The default, specifies that the DS3 line is operating normally
Facility-Loopback	During a facility loopback, the DS3 card returns the signal it receives on the DS3 line.
Local-Loopback	During a local loopback, the DS3 receive path is connected to the DS3 transmit path at the D3 multiplexer. The transmitted DS3 signal is still sent to the network as well.

Using the DS3link command

The DS3Link command is a low-level management tool for use during diagnostic sessions with the T3 card. To open a session with the installed DS3 card, use the Open command.

Then, enter the DS3Link command:

```
> ds3link -option
```

where `-option` is one of the following:

Option	Effect
`-a`	Displays current DS3 line alarms.
`-b on`	Transmits a DS3 Alarm Indication Signal (Blue Alarm).
`-b off`	Stops transmitting a DS3 Alarm Indication Signal (Blue Alarm).
`-c`	Displays and clears line error statistics.
`-d 1 - 7`	Displays current DS2 line state.
`-i on`	Internally loops back the DS3 payload.
`-i off`	Halt internal loop back.
`-l on`	Externally loops back the DS3 payload.

Option	Effect
`-l` off	Halt external loop back.
`-s`	Displays line error statistics without clearing.
`-t`	Toggles debug output.
`-?`	Displays this summary.

To display alarms on the line enter the following:

```
> ds3link -a
   Loss of Signal:            false
   Out of Frame:              false
   Alarm Indication Signal:   false
   Idle Signal:               false
   Yellow Signal:             false
   In Red Alarm:              false
   C-bit parity framing:      false
```

A value of `true` for C-bit parity framing would not indicate an alarm state but that the far end is using C-bit parity.

To display and clear line error statistics enter the following:

```
> ds3link -c
   Line Code Violations:    2136611
   Framing Errors:          67279
   Excessive Zeros:         2098353
   P-bit Parity Errors:     217318
   C-bit Parity Errors:     0
   Far End Block Errors:    0
   DS2 1 Framing Errors:    8415
   DS2 2 Framing Errors:    8415
   DS2 3 Framing Errors:    8415
   DS2 4 Framing Errors:    8415
   DS2 5 Framing Errors:    8415
   DS2 6 Framing Errors:    8415
   DS2 7 Framing Errors:    8415
   Statistics cleared.
```

To display the line state of the third DS2 enter the following:

```
> ds3link -d 3
State of DS2 3:
Out of Frame:              false
Alarm Indication Signal:   false
Yellow Signal:             false
In Red Alarm:              false
Reserved Bit:              false
```

To perform an external loopback test, use the `-l` option as follows:

```
> ds3link -l on
```

To deactivate a DS3 loopback useth the `-l` option.

```
> ds3link -l off
 DS3  loopback deactivated
```

Adminstering OC3-ATM cards

The status profiles on the VT100 interface allow you to perform diagnostics on the OC3-ATM card by viewing available lines, each line's status and any errors on that line. The OC3Framer, ATMDumpCall, and OAM commands allow you to perform diagnostics on the OC3-ATM card.

Interpreting the status windows

The 10-100 and 20-100 status windows display the overall status of the OC3 lines. You can also view this information on the OC3-ATM card status lights. Figure 3-1 shows an example status window.

Figure 3-1. OC3 status windows

```
+--------------------+ +--------------------+
|10-100    OC3-SMF   | |20-100    OC3-UTP   |
|ACT OOF RED YEL AIS | |ACT OOF RED YEL AIS |
| *   -   -   -   -  | | *   -   -   -   -  |
|                    | |                    |
+--------------------+ +--------------------+
```

The status windows include the following codes:

Code	Indicator	Description
ACT	*	Active. The OC3 interface is enabled and has not detected any error conditions.
	-	The OC3 interface is not enabled.
OOF	*	Out of Frame. The OC3 interface is out of frame alignment or there is no physical link.
	-	If the line is enabled, the OC3 interface is operating normally.
RED	*	Red alarm. The OC3 interface is experiencing loss of receive signal or there is no physical link.
	-	If the line is enabled, the OC3 interface is operating normally.
YEL	*	Yellow alarm. The OC3 interface has detected Far End Receive Failure indication transmitted from the other side, or there is no physical link.
	-	If the line is enabled, the OC3 interface is operating normally.
AIS	*	Alarm indication Signal. The local device has received an alarm indication signal or there is no physical link. Also known as a blue alarm.

Code	Indicator	Description
	-	If the line is enabled, the OC3 interface is operating normally.

Figure 3-2, Figure 3-3 and Figure 3-4are examples of OC3 status windows and what they indicate.

Figure 3-2. Status window, lines are disabled.

```
+--------------------+ +--------------------+
|10-100    OC3-SMF   | |20-100    OC3-UTP   |
|ACT OOF RED YEL AIS | |ACT OOF RED YEL AIS |
| -   -   -   -   -  | | -   -   -   -   -  |
|                    | |                    |
+--------------------+ +--------------------+
```

Figure 3-3. Status window, lines are enabled without physical link.

```
+--------------------+ +--------------------+
|10-100    OC3-SMF   | |20-100    OC3-UTP   |
|ACT OOF RED YEL AIS | |ACT OOF RED YEL AIS |
| -   *   *   *   *  | | -   *   *   *   *  |
|                    | |                    |
+--------------------+ +--------------------+
```

Figure 3-4. Status window, lines are enabled, with physical links present and in sync.

```
+--------------------+ +--------------------+
|10-100    OC3-SMF   | |20-100    OC3-UTP   |
|ACT OOF RED YEL AIS | |ACT OOF RED YEL AIS |
| *   -   -   -   -  | | *   -   -   -   -  |
|                    | |                    |
+--------------------+ +--------------------+
```

Accessing the diagnostic interface

The OC3 diagnostic commands are available from the Diagnostic interface. To access the diagnostic interface, Press Control-D, then select `D=Diagnostics`:

```
DO...
 >0=Esc
  1=Dial
  P=Password
  E=Termsrv
  D=Diagnostics
```

The diagnostic interface the appears, indicated by the > prompt. To exit the Diagnostic interface and return to the configuration interface, enter Quit.

Using the OC3Framer command

The OC3Framer command is a low-level management tool for use during diagnostic sessions with the OC3-ATM card.

From the diagnostic interface, enter the OC3Framer command:

```
> oc3framer slot -option
```

where *slot* is the slot the OC3 card is installed in (either Slot 1 or Slot 2) and *-option* is one of the following:

Option	Effect
-t	Toggles debug output.
-d	Dumps ATM framer chip status information. Some of the information this command displays is also available from the status lights on the card.
-s	Synchronizes to the OC3-ATM profile. The DSL Terminator automatically rereads the line configuration whenever it comes up.
-c	Clears the error counters.
-?	Displays this option summary.

For example, to view overall status information about the OC3-ATM line in slot 1, specify slot 1 and enter the OC3Framer command with the -d option:

```
> oc3framer 1 -d

Framer is Enabled

LOS_LED    : Off
LOF_LED    : Off
AIS_LED    : Off
OOF_LED    : Off
ACTIVE_LED : On

RSOP_BIP   Error Counter: 3
RLOP_BIP   Error Counter: 107
RLOP_FEBE  Error Counter: 74
RPOP_BIP   Error Counter: 74
RPOP_FEBE  Error Counter: 50
RACP_CHCS  Error Counter: 0
RACP_UCHCS Error Counter: 7
RACP_RX    Cell Counter : 0
TACP_TX    Cell Counter : 0
```

The OC3Framer command output includes the following fields:

State	Description
LOS_LED	On indicates the OC3 line is experiencing a loss of signal.
LOF_LED	On indicates the OC3 line is experiencing a loss of framing.

State	Description
AIS_LED	On indicates the card is receiving alarm indication signal.
OOF_LED	On indicates the near end is in an out of frame condition.
ACTIVE_LED	On indicates multipoint established.

The remaining output fields indicate the errors on the OC3 line:

Field	Description
RSOP_BIP Error Counter	Number of Receive Section Overhead Processor (RSOP) Bit Interleaved Parity (BIP)-8 errors. The RSOP synchronizes and descrambles frames and provides section-level alarms and performance monitoring.
RLOP_BIP Error Counter	Number of Receive Line Overhead Processor (RLOP) BIP-8 errors. The RLOP is responsible for line-level alarms and for monitoring performance.
RLOP_FEBE Error Counter	Number of RLOP Far-End-Block errors (FEBE).
RPOP_BIP Error Counter	Number of Receive Path Overhead Processor (RPOP) BIP-8 errors. The RSOP interprets pointers and extracts path overhead and the synchronous payload envelope. It is also responsible for path-level alarms and for monitoring performance.
RPOP_FEBE Error Counter	Number of RPOP Far-End-Block errors (FEBE).
RACP-CHCS Error Counter	Number of Receive ATM Cell Processor (RACP) Correctable Header Check Sequence (CHCS) errors. The RACP delineates ATM cells and filters cells based on their idle or unassigned status or HCS errors. It also descrambles the cell payload.
RACP-UCHCS Error Counter	Number of RACP Uncorrectable Header Check Sequence (UCHCS) errors.
RACP-Rx-Cell-Count	Receive ATM Cell Processor (RACP) received cell count.
TACP-Tx-Cell-Count	Transmit ATM Cell Processor (TACP) transmited cell count.

Using the ATMDumpCall command

The ATMDumpCall command is a low-level management tool for use during diagnostic sessions with the OC3-ATM card. It allows you to view the ATM call blocks, which contain information about outgoing calls.

From the diagnostic interface, enter the ATMDumpCall command:

```
> atmdumpcall -option
```

where ***-option*** is one of the following:

Option	Effect
`-a`	Display all ATM call blocks, even those that are inactive.

Option	Effect
`-l`	Display active ATM lines.
`-u`	Display in-use ATM call blocks.

For example, to view all ATM call blocks, enter the ATMDumpCall command with the `-a` option:

```
> atmdumpcall -a
ATM Call Block Table:
Addr.     Index Active  callID  routeID State     Vpi/Vci     Prof_Name  Sess_Up
8036BA48  0     1       1       1       CONNECTED 1/42        atmw       Yes
8036BA90  1     0       65535   0       INACTIVE  0/0           -        No
8036BAD8  2     0       65535   0       INACTIVE  0/0           -        No
8036BB20  3     0       65535   0       INACTIVE  0/0           -        No
8036BB68  4     0       65535   0       INACTIVE  0/0           -        No
.
.
.
E00C5868  62    0       65535   0       INACTIVE  0/0           -        No
E00C58AC  63    0       65535   0       INACTIVE  0/0           -        No

ATM Free Blocks: 359
ATM Used Blocks: 1
```

Using the OAM command

The OAM command sends ATM Operation-And-Maintenance (OAM) loopback cells on an ATM interface, to obtain information about the results of the looped cells.

From the diagnostic interface, enter the OAM command:

```
>oam -e|c|l|p slot port vpi vci arguments
```

where the command line arguments are one of the following:

Option	Description
`-e`	Displays the OAM entries for each opened VCC. (You must first toggle on the debug display using the `-p` option.)
`-c`	(Continuity). Transmit an OAM continuity cell every second on the specified VPI/VCI. This option and the `-l` option are mutually exclusive, and one of them must be specified on the command line.
`-l`	(Loopback). Transmit OAM loop cells. This option and the `-l` option are mutually exclusive, and one of them must be specified on the command line.
`-p`	Toggles debug output.
`slot`	Specifies the slot in which the OC3 card is located.
`port`	Specifies the OC3 port to loop back.

Option	Description
vpi	Specifies the Virtual Path Identifier on which to transmit the looped-back cells.
vci	Specifies the Virtual Channel Identifier on which to send the looped-back cells.
arguments	Arguments can be any of the following: + activates a continuity test (used only with the -c option) - deactivates a continuity test (used only with the -c option) n specifies the number of cells to transmit during a loopback test (used only with the -l option) e (End-to-End). Transmit an end-to-end OAM loop cell, to be looped by the user connection point. This option and the -s option are mutually exclusive, and one of them must be specified on the command line. (Used only with the -l or -c options.) s (Segment). Transmits a segment OAM loop cell, to be looped by the first network connection point. This option and the -e option are mutually exclusive, and one of them must be specified on the command line. (Used only with the -l or -c options)
slot	Specifies the slot in which the OC3 card is located.
port	Specifies the OC3 port to loop back.
vpi	Specifies the Virtual Path Identifier on which to transmit the looped-back cells.
vci	Specifies the Virtual Channel Identifier on which to send the looped-back cells.

Following is an example OAM command line that activates a loopback. It is in the form

```
oam -l slot port vpi vci e|s n
```

For example:

```
>oam -l 2 1 2 12 e 24
OAM: received our loop #1
OAM: received our loop #2
..
...
```

Following is an example OAM command line that activates a continuity check. It is in the form

```
oam -c slot port vpi vci e|s +|-
```

For example, the command:

```
>oam -c 2 1 2 12 e +
```

activates the check. The command:

```
>oam -c 2 1 2 12 e -
```

deactivates the check.

Looping back the OC3-ATM line

For diagnostics, you might want to loopback the OC3 interface by using the Loopback parameter in the Net/OC3-SMF-ATM (Net/OC3-UTP-ATM)> Line Diag profile. As long as the interface is looped back, normal data traffic is interrupted. The Loopback parameters supports the following options:

Value	Description
None	The default, specifies that the OC3 line is operating normally.
Remote	During a facility loopback, the OC3 card returns the signal it receives on the OC3 line.
Local	During a local loopback, the OC3 receive path is connected to the OC3 transmit path at the D3 multiplexer. The transmitted OC3 signal is still sent to the network as well.

You can view the line statistics by using the OC3Framer command. For information about this command, see “Using the OC3Framer command” on page 3-11.

To do a loopback, proceed as in the following example:

1 Open the Net/OC3-SMF-ATM > Line Diag menu:

```
10-200 Line Diag
10-201 Loopback
```

2 Select Loopback and press Enter:

```
Loopback
 >0=ESC
  1=Set
```

3 Select `1=Set` and press Enter to start the loopback.

4 To end the loopback, press Escape:

```
Loopback
  0=ESC (deactivate)
```

Diagnostic Commands

4

The VT100 interface diagnostic commands are usedfor WAN lines and ports. To use these commands, you must have sufficient permissions in the active Security profile. With these commands you can store and save a configuration, reset the unit, start terminal sessions, and retrieve RADIUS information.

Using sys diag commands

The DSL Terminator provides the following system diagnostic commands which appear in the System > Sys Diag menu:

```
System
   Sys Diag
      Restore Cfg
      Save Cfg
      Sys Reset
      Upd Rem Cfg
```

To enter a command, highlight the command in the Sys Diag menu and press Enter.

Note: To use these commands, the operator must have sufficient permissions in the active Security profile.

System diagnostic command reference

This section descibes each of the system diagnostic commands.

Restore Cfg

The Restore Cfg command restores a DSL Terminator configuration that was saved with the Save Cfg parameter or transfers the profiles to another DSL Terminator. Because the Save Cfg command does not save passwords, the Restore Cfg command does not restore them. Follow these instructions to restore your configuration from backup:

1 Verify that the Upload and Edit Security permissions are enabled in the active Security profile.

2 Verify that the Term Rate parameter in the System profile is set to 9600.

3 Verify that your terminal-emulation program has a disk-capture feature and an autotype feature, and that its data rate is set to 9600 bps.

4 Connect the backup device to the DSL Terminator's control port.

5 Highlight Restore Cfg and press Enter.

6 When the `Waiting for upload data` prompt appears, turn on the autotype function on your emulator and supply the filename of the saved DSL Terminator data.

7 Verify that the configuration data is going to your terminal-emulation screen and is being restored to the target DSL Terminator.

The restore process is complete when the message `Upload complete--type any key to return to menu` appears on your emulator's display.

Save Cfg

The Save Cfg command saves the DSL Terminator configuration to a file. It does not save Security profiles or passwords.

Note: Using the Save Cfg command to save the configuration and then restoring it from the saved file clears all passwords.

To save your configuration, proceed as follows:

1 Verify that the Download permission is enabled in the active Security profile.

2 Verify that the Term Rate parameter in the System profile is set to 9600.

3 Verify that your terminal-emulation program has a disk-capture feature and an autotype feature, and that the data rate is set to 9600 bps or lower.

4 Connect the backup device to the DSL Terminator's control port.

5 Turn on the autotype function on your emulator, and start the save process by pressing any key on the emulator.

6 Highlight Save Cfg and press Enter.

7 Verify that configuration data is being echoed to the terminal-emulation screen and that the captured data is being written to a file on your disk.

The save process is complete when the message `Download complete--type any key to return to menu` appears on your emulator's display. The backup file is an ASCII file.

8 Turn off the autotype feature.

Sys Reset

The Sys Reset command restarts the DSL Terminator and clears all calls without disconnecting the device from its power source. The DSL Terminator logs out all users and returns user security to its default state. In addition, the DSL Terminator performs Power-On Self Tests (POSTs) when it restarts. The POSTs are diagnostic tests.

A system reset of an DSL Terminator causes momentary loss of T1 framing (that is, the data-encapsulation format), and the T1 line might shut down. The feedback from the DSL Terminator to the switch will be incorrect until T1 framing is reestablished.

To perform a system reset, proceed as follows:

1. Highlight System Reset and press Enter.

   The DSL Terminator prompts you to confirm that you want to perform the reset.

2. Confirm the reset.

   The POST display appears. If you do not see the POST display, press Ctrl-L. These messages may be displayed:

```
OPERATOR RESET:  Index: 99   Revision: 5.0a
   Date: 03/04/1997.       Time: 22:32:23
   MENU Reset from unknown in security profile 1.
SYSTEM IS UP:  Index: 100   Revision: 5.0a
   Date: 03/04/1997.       Time: 22:33:00
```

   The DSL Terminator checks system memory, configuration, installed modules, and T1 connections. The alarm relay remains closed while the POST is running and opens upon successful completion of the test, at which time the following message appears:

```
Power-On Self Test PASSED
Press any key...
```

3. Press any key to display the Main Edit Menu.

Term Serv

The Term Serv command starts a terminal-server session. The system displays the terminal-server command-line prompt (by default, `ascend%`). For information about the terminal-server commands, enter a question mark at the prompt. For more details about the terminal-server interface, see the *Network Configuration Guide* or *Reference* for your DSL Terminator.

Upd Rem Cfg

The Upd Rem Cfg (Upload Remote Configuration) command opens a connection to a RADIUS server to upload the DSL Terminator terminal-server banner, list of Telnet hosts, IP static routes, IP address pool, and other configuration information from the RADIUS user file. The DSL Terminator retrieves configuration from RADIUS at system startup or by use of this command.

When you highlight Upd Rem Cfg and press Enter, the DSL Terminator opens a connection to the RADIUS server and uploads the configuration information.

When you upload this remote configuration information, note the following:

- The DSL Terminator reads Dialout-Framed-User entries with the password `ascend`.
- The Upd Rem Cfg command does not update the terminal-server banner or list of Telnet hosts if the Remote Conf parameter is set to No.
- If the Ascend-Authen-Alias attribute is defined in RADIUS, the Upd Rem Cfg command also updates the DSL Terminator system name used when establishing PPP calls.

VT100 Interface Status Windows

5

Using the status windows

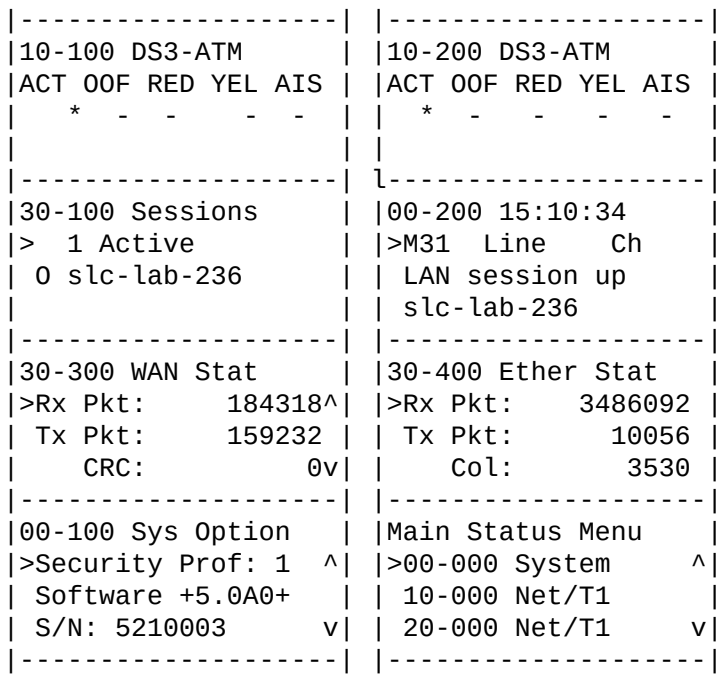
The right side of the screen in the DSL Terminator configuration interface displays eight status windows (Figure 5-1). The status windows provide a great deal of read-only information about what is currently happening in the DSL Terminator.

This section provides an overview of the information contained in the eight windows that are displayed by default, and shows you how to replace a default window with a status window of your choice. Following are the parameters for customizing the display:

```
System
   Sys Config
      Status 1=10-100
      Status 2=10-200
      Status 3=50-100
      Status 4=00-200
      Status 5=50-300
      Status 6=50-400
      Status 7=00-100
     Status 8=00-000
```

The Status numbers 1 through 8 refer to the status-window positions, which start with 1 in the upper left and continue with 2 in the upper right, and so forth. For details about each parameter, see the *DSL Terminator Reference* .

Figure 5-1. Status windows



Navigating the status windows

To make a status window active, press the Tab key until that window is highlighted by a thick border. The Tab key moves the active window in sequence from left to right, top to bottom, and then returns to the Main Edit window (the menu).

To scroll the selections within a status window, Tab to the window, then use the Up Arrow or the Down Arrow key to scroll the window. To access a submenu, use the Right Arrow key, and to return to the original menu use the Left Arrow key.

Some of the status windows contain more information than can be displayed in the small window. A lowercase v in the lower-right corner of a window, indicates that more information is available. You can scroll through additional information if you make the window active.

Default status window displays

You can set the Status parameters in the System profile to specify which status windows are displayed when the DSL Terminator powers up. For descriptions of all of the codes and information that can be displayed in each window, see “Status-window reference in alphabetic order” on page 5-5.

Note: Depending on your DSL Terminator configuration, some of these status windows will appear by default and some may not. If a status window does not appear by a default, each of the descriptions below instruct you how to display the menu from any status window. If the status window described is already displayed on your VT100 interface, all you may want to do is scroll through the submenus to view its contents.

Line status windows

Slot 1 and slot 2 contain the line interface cards. The DSL Terminator can be equipped with ATM-DS3, ATM-OC3, UDS3 or T1 cards. To display the Line Status window, tab to status window 1 or 2 (Figure 5-2), then use the arrow keys to access the status of the desired line interface card. For example:

Figure 5-2. Line Status Windows

```
|--------------------| |--------------------|
|10-100 DS3-ATM      | |10-200 DS3-ATM      |
|ACT OOF RED YEL AIS | |ACT OOF RED YEL AIS |
|   *  -  -    -  -  | |  *  -   -   -   -  |
|                    | |                    |
|--------------------| l--------------------|
```

SeeChapter 3, “Administering Slot Cards,” for more information about status window information available in Line status windows.

Session and system status windows

The system itself is assigned slot number 0, and the slot number 9 is assigned to the built-in Ethernet port. By default, the next two status windows show active routing sessions on Ethernet and up to 32 log messages related to the system itself:

Figure 5-3. Active Sessions and Messages Windows

```
|--------------------| l--------------------|
|30-100 Sessions     | |00-200 15:10:34     |
|>  1 Active         | |>M31  Line    Ch    |
| O slc-lab-236      | | LAN session up     |
|                    | | slc-lab-236        |
|--------------------| |--------------------|
```

The Sessions window shows the number of active bridging/routing and modem (terminal server) sessions. When this window is active, you can scroll down to see the name, address, or Calling Line ID (CLID) of each connected device. Each line starts with a one-character session-status indicator. For example, O means online. For terminal-server sessions, the modem number is identified.

You can also display the Sessions window, by tabbing to any status window, and using the arrow keys to access the Ethernet > Sessions window.

The system message log provides a log of up to 32 of the most recent system events. To display the System Message Log window, tab to any status window, then use the arrow keys to access the System > Message Log window.

Use an arrow key to scroll up (previous messages) or down (later messages). The Delete key clears all the messages in the log. The message log window is organized as follows:

- The first line shows the menu number and the time the most recently logged event occurred.
- The second line identifies the log entry number (M31) and, if applicable, the line and channel on which the event occurred.

- The third line contains the text of the message. For example:
  - Call Terminated (An active call disconnected normally.)
  - LAN session up (An incoming connection has been established.)
  - No Connection (The remote device did not answer the call.)
- The fourth line contains a message qualifier, such as a name or phone number that qualifies the message displayed.

WAN and Ethernet status windows

By default, the fifth and sixth status windows (Figure 5-4) show statistics about each active WAN link and the Ethernet interface. For example:

Figure 5-4. WAN and Ethernet Statistics Windows

```
|--------------------| |--------------------|
|30-300 WAN Stat     | |30-400 Ether Stat   |
|>Rx Pkt:     184318^| |>Rx Pkt:    3486092 |
| Tx Pkt:     159232 | | Tx Pkt:      10056 |
|    CRC:          0v| |    Col:       3530 |
|--------------------| |--------------------|
```

The WAN Stat window shows the current count of received frames, transmitted frames, and frames with errors for each active WAN link and for the entire WAN. When this window is active, you can scroll down to see the statistics for each link. The first line of each per-link count shows the name, IP address, or MAC address of the remote device.

You can also display the WAN Stat window, by tabbing to any status window and using the arrow keys to access the Ethernet > WAN Stat window.

The Ether Stat window shows the current count of received frames, transmitted frames, and frames with errors at the Ethernet interface. To display the Ether Stat window, tab to any status window, then use the arrow keys to access the Ethernet > Ether Stat window.

Sys Option and Main Status Menu windows

The bottom two status windows are usually the Sys Option window, which contains management information about the DSL Terminator, and the Main Status Menu window. For example:

Figure 5-5. Sys Option and Main Status Menu Windows

```
|--------------------| |--------------------|
|00-100 Sys Option   | |Main Status Menu    |
|>Security Prof: 1  ^| |>00-000 System     ^|
| Software +5.0A0+   | | 10-000 Net/T1      |
| S/N: 5210003      v| | 20-000 Net/T1     v|
|--------------------| |--------------------|
```

The Sys Options window shows which Security profile is active, which Lucent software version is running, the unit's serial number (S/N). Additionally, it can list a variety of hardware or software options. It also displays a system uptime value, which is updated every few

seconds to show the number of days, hours, minutes, and seconds the DSL Terminator has been operating. For example:

```
Up: 12:17:18:26
```

When the Sys Options window is active, you can use the arrow keys to scroll down and display the list of system options. For example, some system options that can appear are the software load name, various installed-software options (such as Frame Relay, AIM, and BONDING), and the AuthServer and AcctServer options, which specify the IP addresses of the RADIUS (or TACACS) authentication server and the RADIUS accounting server.

You can also display the System Options window, by tabbing to any status window, then using the arrow keys to access the System > Sys Option window.

The last status window contains the Main Status Menu, a hierarchical menu that contains an entry for each line or installed card in the DSL Terminator. The structure of the Main Status Menu exactly follows the Main Edit Menu (the top-level configuration menu).

When the window that displays the Main Status Menu is active, the menu works like the Main Edit Menu. Use the arrow keys to scroll to a particular status menu. Then press the Enter key to open that menu and the Escape key to close it.

Specifying which status windows appear

You can specify which status windows the VT100 interface displays. The total number of status window that can be displayed is limited to eight. You can use the system configuration profile to choose which status windows are displayed in the eight available positions.For details about the windows you can choose to display and the information in each one, see “Status-window reference in alphabetic order” on page 5-5.

To specify which status windows appear on the VT100 interface, proceed as follows:

1. From the Main Edit Menu, select System > Sys Config.
2. Using the down arrow key, navigate to the list of eight status window parameters `Status 1 through Status 8` and select the desired status parameter.
3. Press the right arrow key and enter the number of the status window that you wish to display in that position.

   Note: Every menu and submenu has an identifying number, for example, 20-100, or 20-200. You can scroll through the Main Status Menu to get the identifying status numbers.
4. Save and close the System profile.

When the DSL Terminator resets, the status windows appear with the new selections.

Status-window reference in alphabetic order

This section describes in detail the contents of each status window. It lists the windows in alphabetic order.

CDR window

Call Detail Reporting (CDR) provides a database of information about each call, including date, time, duration, called number, calling number, call direction, service type, associated inverse-multiplexing session, and port. Because the network carrier bills for bandwidth on an as-used basis, and bills each connection in an inverse multiplexed call separately, you might want to use CDR to understand and manage bandwidth usage and the cost of each inverse-multiplexed session.

You can arrange the information to create a wide variety of reports, which can be based on factors such as individual call costs, inverse-multiplexed WAN-session costs, costs on an application-by-application basis and bandwidth usage patterns over specified time periods. With a better understanding of your bandwidth usage patterns, you can make any necessary adjustments to the ratio of switched to nailed bandwidth between network sites.

Like the DSL Terminator message logs, CDR shows the most recent session event. The DSL Terminator generates new CDR messages as events occur. However, unlike a log, the DSL Terminator does not store past CDR events. The CDR window is primarily a source of data captured by external devices.

To display the CDR window, tab to any status window, then use the arrow keys to access the System > CDR window.

Following is a sample four-line CDR display:

```
00-400 CDR
 93:05:28:10:33:52
 OR 025 384KR 02-01
 15105551212
```

The first line displays the status-window number and title.

The second line displays the time at which the event occurred, in the following format:

year:*month*:*day*:*hour*:*minute*:*second*

The third line displays the following items of information about the CDR event in the order shown:

Item	Description
CDR event description	Consists of one of the following abbreviations: • OR—Originated (outgoing call) • AN—Answered (incoming call) • AP—Assigned to Port or module (incoming call) • CL—Cleared • OF—Overflowed All events except OF are associated with calls. OF indicates that the CDR buffer overflowed because events occurred faster than the DSL Terminator could report them.

Item	Description
CDR event ID	The DSL Terminator creates a new event ID for every DS0 channel originating a connection. The event ID number, range, from 0 to 255. Events after 255 start the count again at 0. In addition, CDR creates a new event ID for every change in a channel's status. Because a DSL Terminator call can consist of several channels, the DSL Terminator can generate multiple CDRs for every change in call status.
Data service in use	Indicates the data service, using values nearly identical to those available to the Data Svc parameter in the Call profile. The only difference is that the Data Svc values 384K/H0 and 1536K correspond to the CDR data service values 384K and 1536KR, respectively.
Slot-port address	The address at which event occurred. For example, if the event occurred on the first port of a Host/6 card installed in slot 3, the slot-port address is 03-01.

The fourth line displays either the dialed or called-party phone number. If the event description on line 3 is OR (outgoing call), the number dialed appears. If the event description on line 3 is AN (incoming call), the called-party number appears. To get the called-party number on incoming calls, you must have DNIS service from your WAN provider. In some cases, the called-party number is not delivered, (for example, when the DSL Terminator is behind some types of PBX).

For related information, see the Data Svc parameter in the DSL Terminator *Reference.*

Dyn Stat window (dynamic status)

The Dynamic Status (Dyn Stat) window shows the name, quality, bandwidth, and bandwidth utilization of each online, multichannel, PPP connection with dynamic bandwidth management. To display the Dyn Stat window, tab to any status window, then use the arrow keys to access the Ethernet > Dyn Stat window.

Following is the Dyn Stat display for an Ethernet module in slot 9:

```
90-500 Dyn Stat
 Qual Good 00:02:03
 56K     1 channels
 CLU  12%  ALU  23%
```

Note: Press the Down Arrow key to see additional online multichannel PPP connections.

The first line of the Dyn Stat window shows the window number and the name of the current Connection profile. If no connection is currently active, the window name appears instead.

The second line lists the quality of the link and the amount of time the link has been active. When a link is online more than 96 hours, the DSL Terminator reports the duration in number of days. The link quality can have one of the following values:

- Good—The current rate of CRC errors is less than 1%.
- Fair—The current rate of CRC errors is between 1% and 5%.
- Marg—The current rate of CRC errors is between 5% and 10%.
- Poor—The current rate of CRC errors is more than 10%.

- N/A—The link is not online.

The third line of the Dyn Stat window shows the current data rate in Kbps, and how many channels this data rate represents.

The fourth line displays the following values:

- CLU—Current Line Utilization. The percentage of bandwidth currently being used by the call for transmitted data, divided by the total amount of bandwidth available.
- ALU—Average Line Utilization. ALU is the average amount of available bandwidth used by the call for transmitted data during the current history period as specified by the Sec History and Dyn Alg parameters.

Ether Opt window

The Ethernet Options (Ether Opt) window lists the type of Ethernet interface specified in the Ethernet I/F parameter, and its MAC address. To display the Ether Opt window, tab to any status window, then use the arrow keys to access the Ethernet > Ether Opt window.

Following is an example of an Ether Opt display for an Ethernet module in slot 9:

```
90-600 Ether Opt
>I/F: COAX
 Adrs: 00c07b322bd8
```

The interface type may be AUI, UTP, or COAX. The MAC address is a 6-byte hexadecimal address assigned to the Ethernet controller by the manufacturer. For related information, see the entry for the Ethernet I/F parameter in the *DSL Terminator Reference.*

Ether Stat window

The Ethernet Status (Ether Stat) window shows the number of Ethernet frames received and transmitted and the number of collisions at the Ethernet interface. To display the Ether Stat window, tab to any status window, then use the arrow keys to access the Ethernet > Ether Stat window.

For example, the following screen shows the Ether Stat display for an Ethernet module in slot 9:

```
90-400 Ether Stat
>Rx Pkt:      106
    Col:        0
 Tx Pkt:      118
```

The screen shows the following fields:

- Rx Pkt—Number of Ethernet frames received on the Ethernet interface
- Col—Number of collisions detected at the Ethernet interface
- Tx Pkt—Number of Ethernet frames transmitted over the Ethernet interface

The counts return to 0 (zero) when the DSL Terminator is switched off or reset. Otherwise, the counts continuously increase, up to the maximum allowed by the display.

Ethernet window

The Ethernet window is a subwindow of the Main Status Menu window. The Ethernet window itself has subwindows which display the status of the Ethernet interface. When you choose Ethernet from the Main Status Menu window, the following menu appears:

```
50-000 Ethernet
 50-100 Sessions
 50-200 Routes
 50-300 WAN Stat
```

FR Stat window

The Frame Relay Status (FR Stat) window shows the status of each online link defined in a Frame Relay profile. To display the FR Stat window, tab to any status window, then use the arrow keys to access the Ethernet > FR Stat > *any active Frame Relay connection* window.

The window shows the number of packets received and transmitted on the Frame Relay connection. It also shows the number of frames received with CRC errors.

Line Stat windows

The Line Status (Line Stat) windows (Line 1 Stat and Line 2 Stat) show the dynamic status of each WAN line, the condition of its electrical link to the carrier, and the status of its individual channels. To display the Line Status window, tab to any status window, then use the arrow keys to access the Net/T1 > Line *N* Stat (or Net/E1 >Line *N* Stat) window.

Following is an example of a Line Stat window display:

```
10-100 1234567890
L1/LA  ----------
   12345678901234
   -------------s
```

The first line of a Line Stat window shows the window number followed by ten columns for channels 1 through 10 (0).

The second line begins with the line number, followed by the link status, which is indicated by one of the two-character abbreviations listed in Table 5-1. Following the link status is a single character that indicates the first channel's status. Table 5-2 lists the channel-status indicators.)

The third line has column headers for the remaining channels.

The fourth line continues where the second line left off, showing the status of the remaining channels.

Table 5-1. T1/E1 link-status indicators

Link status	Description
LA	Link active. The line is active and physically connected.

Table 5-1. T1/E1 link-status indicators (continued)

Link status	Description
RA	Red Alarm/Loss of Sync. The line is not connected, improperly configured, experiencing a very high error rate, or is not supplying adequate synchronization. The Alarm LED lights when the line is in this state.
YA	Yellow Alarm. The DSL Terminator is receiving a Yellow Alarm pattern. The Yellow Alarm pattern is sent to the DSL Terminator to indicate that the other end of the line cannot recognize the signals the DSL Terminator is transmitting. The Alarm LED lights when the line is in this state.
1S	Keep alive (all ones). Also known as Blue Alarm. A signal is being sent from the T1 PRI network to the DSL Terminator to indicate that the T1 PRI line is currently inoperative. The Alarm LED lights when the line is in this state.
DS	Disabled link. The line is physically connected, but you have disabled the line in the Line *N* profile.

A single character represents the status of each channel in the line, as described in Table 5-2:

Table 5-2. T1 channel status indicators

Channel status	Description
.	Not available. The channel is not available because the line is disabled, has no physical link, or does not exist, or because the channel is set to Unused in the Ch *N* parameter of the Line *N* profile.
*	Current. The channel is connected in a current call.
-	Idle. The channel is currently idle (but in service).
d	Dialing. The DSL Terminator is dialing from this channel for an outgoing call.
r	Ringing. The channel is ringing for an incoming call.
n	Nailed. The channel is marked Nailed in the Line *N* profile.

Note: If the DSL Terminator is configured for Drop-and-Insert functionality, and a Red Alarm (RA) or Loss of Sync condition is detected, the failure is conveyed to the device by sending an all ones (A1S) over Line 2. During the time this failure is active, devices connected to Line 2 cannot place calls.

Message Log windows

You can display the Message Log window for the system itself. Each message log displays up to 32 of the most recent system events the DSL Terminator has recorded. When you select the Message Log option, the most recent message appears. The message logs update dynamically. Press the Up-Arrow key to display the previous entry. Press the Down Arrow key to display the next entry.

To display the Message Log window, tab to any status window, then use the arrow keys to access the Host/Dual > Port*N* Stat > Messages window.

System message logs

Access the Message Log window for the system for a log of system events by selecting it in the System status window. The following example shows a Message Log entry generated by an incoming call not yet assigned to an AIM port:

```
00-200 11:23:55
>M31 Line 1 Ch 07
 Incoming Call
 MBID 022
```

The first line shows the status window number and the time the event occurred.

The second line identifies a log entry number (M00 to M31) and, if applicable, the line and channel on which the event occurred.

The third line contains the text of the message (as described in Table 5-3 on page 11).

The fourth line contains connection-specific messages (as described in Table 5-5 on page 14).

Log messages

Table 5-3 shows the informational messages that can appear in the Message Log window:

Table 5-3. Informational log messages

Message	Description
Added Bandwidth	The DSL Terminator has added bandwidth to an active call.
Assigned to port	The DSL Terminator has assigned an incoming call to an AIM port, a digital modem, the packet-handling module, or the terminal server.
Call Terminated	An active call was disconnected normally, although not necessarily by operator command.
Callback Pending	The DSL Terminator is waiting for callback from the remote end.
Ethernet up	The Ethernet interface has been initialized and is running.
Handshake Complete	The handshake was completed, but no channels were added. Either a user entered the DO R command to resynchronize channels, or an attempt to add channels to an inverse-multiplexing call failed.

Table 5-3. Informational log messages (continued)

Message	Description
Incoming Call	The DSL Terminator has answered an incoming call at the T1 PRI network interface but has not yet assigned the call to an AIM port or to the IP router.
Incomplete Add	An attempt to add channels to an inverse-multiplexing call failed. The DSL Terminator added some channels, but fewer than the number requested. This situation can occur when placing a call. The first channel connects, but the requested base channel count fails.
LAN session down	Appears before Call Terminated if a PPP, MP+, or Combinet session is terminated.
LAN session up	Appears after Incoming Call if a PPP, MP+, or Combinet session is established.
Moved to primary	Some nailed-up channels that the DSL Terminator removed from an FT1-B&O call have been restored because their quality was no longer poor. The fourth line of the Message Log window indicates the number of channels restored.
Moved to secondary	The DSL Terminator has detected some poor- quality nailed-up channels in an FT1-B&O call and has backed up the call on switched channels. The fourth line of the Message Log window indicates the number of channels removed.
Outgoing Call	The DSL Terminator has dialed a call.
Port use exceeded	Call usage for an AIM port has exceeded the maximum specified by either the DS0 Mins or Call Mins parameter in the Port profile.
Removed Bandwidth	The DSL Terminator has removed bandwidth from an active call.
Sys use exceeded	Call usage for the entire system has exceeded the maximum specified by the DSL Terminator DS0 Mins parameter in the System profile.
RADIUS config error	The DSL Terminator has detected an error in the configuration of a RADIUS user entry.
Requested Service Not Authorized	Appears in the terminal-server interface if the user requests a service not authorized by the RADIUS server.

Table 5-4 shows the warning messages that can appear in the Message Log windows.

Table 5-4. Warning log messages

Message	Description
Busy	The phone number was busy when the call was dialed.

Table 5-4. Warning log messages (continued)

Message	Description
Call Disconnected	The call has ended unexpectedly.
Call Refused	An incoming call could not be connected to the specified AIM port, digital modem, packet-handling module, or terminal server because the resource was busy or otherwise unavailable.
Dual Port req'd	The call could not be placed because one or both ports of the dual-port pair were not available.
Far End Hung Up	The remote end terminated the call normally.
Incoming Glare	The DSL Terminator could not place a call because it saw an incoming *glare* signal from the switch. Glare occurs when you attempt to place an outgoing call and answer an incoming call simultaneously. If you receive this error message, you have probably selected incorrect settings in the Line *N* profile.
Internal Error	Call setup failed because of a lack of system resources. If this type of error occurs, notify Lucent Customer Service.
LAN security error	Appears after Incoming Call but before Call Terminated if a PPP, MP+, terminal-server, or Combinet session has failed authentication, another session by the same name already exists, or the time-out period for RADIUS/TACACS authentication has been exceeded. For details, see the entry for the Auth Timeout parameter in the DSL Terminator *Reference.*
Network Problem	The call setup was faulty because of problems within the WAN or in the Line *N* profile configuration. The telco might be experiencing a problem.
No Chan Other End	No channel was available on the remote end to establish the call.
No Channel Avail	No channel was available to dial the initial call.
No Connection	The remote end did not answer when the call was dialed.
No Phone Number	No phone number exists in the Call profile being dialed.
No port DSO Mins	No maximum has been specified for the DSL Terminator DS0 Mins or DSL Terminator Call Mins parameter in the Port profile.
No System DSO Mins	No maximum has been specified for the DSL Terminator DS0 Mins parameter in the System profile.
Not Enough Chans	A request to dial multiple channels or to increase bandwidth could not be completed because there were not enough channels available.

Table 5-4. Warning log messages (continued)

Message	Description
Not FT1-B&O	The local DSL Terminator attempted to connect an FT1-B&O call to the remote end, but the call failed because the call type at the remote end was not FT1-B&O.
Remote Mgmt Denied	The DSL Terminator rejected a request to run the remote DSL Terminator by AIM remote management because the Remote Mgmt parameter in the System profile at the remote end is set to `No`.
Request Ignored	The DSL Terminator denied a request to manually change bandwidth during a call because the Call Mgm parameter in the Call profile is set to `Dynamic`. With this setting, the DSL Terminator allows only automatic bandwidth changes.
Wrong Sys Version	The remote-end product version was incompatible with the version of the local DSL Terminator. The software version appears in the Sys Options status window.

Table 5-5 shows connection messages that can appear on the fourth line of the Message Log windows.

Table 5-5. Message indicators

Indicator	Description
MBID *value*	Appears with either the Incoming Call or Assigned to Port (line 3) messages. The first message means an incoming call has been received and the second message means it has been routed to a DSL Terminator port. If you cannot match the MBID value of an incoming call log to the MBID value in an assigned-to-port log, the call disconnected, often because the intended port was busy. MBID also appears in the System log.
Channels	Number of channels added to or removed from a call. Appears with the Added Bandwidth, Removed Bandwidth, Moved to Primary, and Moved to Secondary messages. When Line 3 displays an Outgoing Call, line 4 displays the phone number dialed. In multichannel calls, line 4 displays the phone number for the first connection. Only the phone number appears. The parameter name, Phone Number, does not.
Name	When the message in line 3 is either LAN `session up` or LAN `session down`, line 4 displays the remote end's name. If the session is a Combinet bridging link, the MAC address is displayed. If the session is a PPP link, either the remote end's system name (as specified by the Name parameter in the System profile) or IP address (as specified by the IP Adrs parameter in the Ethernet profile) is displayed. The IP address is displayed only if the system's name is not known.

Table 5-5. Message indicators (continued)

Indicator	Description
CLID	When an incoming call is answered and the calling party number is known, line 4 specifies the CLID. When the CLID appears, the MBID does not.

Net T1 and Net E1 windows

Net/T1 and Net E1 windows are subwindows of the Main Status Menu window. Following are the contents of the Net/T1 window for the base system's T1 PRI interface:

```
10-000 Net/T1
 10-100 Line 1 Stat
>10-200 Line 2 Stat
 10-300 Line Errors
```

Following are the contents of the Net/E1 window for the base system's E1 PRI interface:

```
10-000 Net/E1
 10-100 Line 1 Stat
>10-200 Line 2 Stat
 10-300 Line Errors
```

Net Options window

The Net Options window lists the WAN interface features installed on your DSL Terminator. To display the Net Options window, tab to any status window, then use the arrow keys to access the Net/T1 > Net Options window.

The following screen shows the Net Options window:

```
Net Options
>T1/PRI Network I/F
 2 Network I/F(s)
 Type: CSU/CSU
```

The first line shows the type of physical interface to the WAN. The line can specify either T1/PRI Network I/F.

The second line shows the number of network interfaces associated with the module.

The third line shows whether internal CSUs are installed for the T1 lines. Following are the values that can appear:

- `Type: DSX/DSX`
- `Type: CSU/DSX`
- `Type: DSX/CSU`
- `Type: CSU/CSU`

Routes window

The Routes window displays the current routing table. To display the Routes window, tab to any status window, then use the arrow keys to access the Ethernet > Routes window.

A Routes window initially displays the first route in the table. For example:

```
50-200 Routes
>D: Default
 G: 223.0.100.129
 LOOP Active
```

Note: Press the Down Arrow key to display the next route, or the Up Arrow key to display the previous one.

The second line in a Routes window contains the destination address. The destination can be a network address or the address of a single station. If the route is the default route, the word Default replaces the address.

The third line shows the address of the router.

The fourth line can have one of the values listed in Table 5-6.

Table 5-6. Routes-window values

Value	Description
`LAN Active`	Active route. Has a destination on the local subnet.
`WAN Active`	Active route. Has a destination off the local subnet.
`LOOP Active`	Active route. Has this DSL Terminator as a router and destination. No data packets are propagated.
`LAN Inactive`	Inactive route. Has a destination on the local subnet.
`WAN Inactive`	Inactive route. Has a destination off the local subnet.

A route becomes inactive if taken out of service. Whether a dialed-up link in a route has or has not been connected does not affect the active or inactive status of the route

Sessions window

The Sessions status window indicates the number of active bridging/routing links or remote terminal-server sessions. An online link, as configured in the Connection profile, constitutes a single active session. A session can be PPP or Combinet-encapsulated. The DSL Terminator treats each multichannel MP+ or MP link as a single session. The following screen shows the display when the Ethernet module is installed in Slot 5:

```
50-100 Sessions
>5 Active
 O Headquarters
```

The first line specifies the number and name of the window.

The second line shows the number of active sessions.

The third and all remaining lines use the following format:

`status remote device`

where `status` is a status indicator and `remote device` is the name, address, or CLID of the remote device. Table 5-7 lists the session-status characters that can appear.

Table 5-7. Session status characters

Indicator	Description
Blank	Nothing. No calls exist and no other DSL Terminator operations are being performed.
R	Ringing. An incoming call is ringing on the line, ready to be answered.
A	Answering. The DSL Terminator is answering an incoming call.
C	Calling. The DSL Terminator is dialing an outgoing call.
O	Online. A call is up on the line.
H	Hanging up. The DSL Terminator is clearing the call.

Note: For remote terminal-server sessions, the third and following lines of the Sessions window appear in the format `Modem slot:position`, where `slot` specifies the slot of the active digital modem, and `position` is a number indicating the position of the modem in that slot.

Syslog window

Syslog is not a DSL Terminator status display, but an IP protocol that sends system-status messages to a host computer, known as the Syslog host. The Log Host parameter in the Ethernet profile specifies the Syslog host, which saves the system-status messages in a log file. The messages are derived from two sources—the Message Log display and the CDR display.

Note: See the UNIX man pages about `logger(1)`, `syslog(3)`, `syslog.conf(5)`, and `syslogd(8)` for details of the syslog daemon. The Syslog function requires UDP port 514.

Level 4 and Level 6 syslog messages

The data for Level 4 (warning) and Level 6 Syslog messages is derived from the Message Log displays. Level 4 and Level 6 messages are presented in the following format:

```
ASCEND: slot-n port-n | line-n, channel-n, text-1
ASCEND: slot-n port-n | line-n, channel-n, text-2
```

The device address (slot, port or line, and channel) is followed by two lines of text, which are displayed on lines 3 and 4 of the Message Log window. The device address is suppressed when it is not applicable or unknown.

The line represented by `text-2` specifies the system name and IP address or MAC address of the remote end of a session for the LAN Session Up and LAN Session Down messages in the line represented by `text-1`.

Level 5 Syslog messages

The data for Level 5 (notice) Syslog messages is derived from the CDR display, lines 3 and 4. Level 5 messages are presented in the following format:

ASCEND: *call-event-ID event-description* slot-*N* port-*N* *data-svcK* phone-*N*

Element	Description
call-event-ID	Specifies the event ID in the CDR display.
event description	Description of the CDR event.
slot-*N* port-*N*	Address indicates the AIM port, which is suppressed when it is not applicable or is unknown.
ata-svcK	The data service in use.
phone-N	The phone number.

Example

Because the date, type, and name of a syslog message are added by the Syslog host, the DSL Terminator does not include that data in the message format. Following are sample Syslog entries from a Syslog host:

```
Oct 21 11:18:07 marcsDSL Terminator ASCEND: slot 0\ port 0, line
1, channel 1, \
No Connection

Oct 21 11:18:07 marcsDSL Terminator ASCEND: slot 4\ port 1, Call
Terminated

Oct 21 11:19:07 marcsDSL Terminator ASCEND: slot 4\ port 1, Out-
going Call, 123
```

In this example, three messages are displayed for the system `marcsAscend`. Notice that the back-slash (\) indicates the continuation of a log entry onto the next line.

Disconnect codes and Progress codes

If the Syslog option is set, a Call-Close (CL) message is sent to the `Syslog` daemon whenever a connection is closed. Additional information about the user name, Disconnect code, Progress code, and login host is appended to each CL message. The CL message uses the following format:

*[name,]*c=*xxxx,*p=*yyyy,[ip-addr]*

where

Element	Description
Name	The name of a profile. It can contain up to 64 characters. A name containing more than 64 characters is truncated, and a plus sign is added to the truncated name. The name appears for incoming calls only.
xxxx	The disconnect code.
yyyy	The connection progress code.
ip-addr	The login host's IP address for Telnet and rea TCP connections (if applicable)

Following is a list of disconnect codes and their meanings:

Disconnect code	Description
1	Not applied to any call.
2	Unknown disconnect.
3	Call disconnected.
4	CLID authentication failed.
5	RADIUS timeout during authentication.
6	Successful authentication. DSL Terminator is configured to call the user back.
7	Pre-T310 Send Disc timer triggered.
9	No modem is available to accept call.
10	Modem never detected Data Carrier Detect (DCD).
11	Modem detected DCD, but modem carrier was lost.
12	DSL Terminator failed to successfully detect modem result codes.
13	DSL Terminator failed to open a modem for outgoing call.
14	DSL Terminator failed to open a modem for outgoing call while `ModemDiag` diagnostic command is enabled.
20	User exited normally from the terminal server.
21	Terminal server timed out waiting for user input.
22	Forced disconnect when exiting Telnet session.
23	No IP address available when invoking PPP command.
24	Forced disconnect when exiting raw TCP session.
25	Exceeded maximum login attempts.
26	Attempted to start a raw TCP session, but raw TCP is disabled on DSL Terminator.
27	Control-C characters received during login.
28	Terminal-server session cleared ungracefully.

Disconnect code	Description
29	User closed a terminal-server virtual connection normally.
30	Terminal-server virtual connect cleared ungracefully.
31	Exited from Rlogin session.
32	Establishment of Rlogin session failed because of bad options.
33	DSL Terminator lacks resources to process terminal-server request.
35	MP+ session cleared because no null MP packets received. An DSL Terminator sends (and should receive) null MP packets throughout an MP+ session.
40	LCP timed out waiting for a response.
41	LCP negotiations failed, usually because user is configured to send passwords via PAP, and DSL Terminator is configured to only accept passwords via CHAP (or vice versa).
42	PAP authentication failed.
43	CHAP authentication failed.
44	Authentication failed from remote server.
45	DSL Terminator received Terminate Request packet while LCP was in open state.
46	DSL Terminator received Close Request from upper layer, indicating graceful LCP closure.
47	DSL Terminator cleared call because no PPP Network Core Protocols (NCPs) were successfully negotiated. Typically, there is no agreement on the type of routing or bridging that is supported for the session.
48	Disconnected MP session. The DSL Terminator accepted an added channel, but cannot determine the call to which to add the new channel.
49	Disconnected MP call because no more channels can be added.
50	Telnet or raw TCP session tables full.
51	DSL Terminator has exhausted Telnet or raw TCP resources.
52	For Telnet or raw TCP session, IP address is invalid.
53	For Telnet or raw TCP session, DSL Terminator cannot resolve hostname.
54	For Telnet or raw TCP session, DSL Terminator received bad or missing port number.
60	For Telnet or raw TCP session, host reset.
61	For Telnet or raw TCP session, connection was refused.
62	For Telnet or raw TCP session, connection timed out.
63	For Telnet or raw TCP session, connection closed by foreign host.
64	For Telnet or raw TCP session, network unreachable.
65	For Telnet or raw TCP session, host unreachable.
66	For Telnet or raw TCP session, network admin unreachable.
67	For Telnet or raw TCP session, host admin unreachable.
68	For Telnet or raw TCP session, port unreachable.

Disconnect code	Description
100	Session timed out.
101	Invalid user.
102	Callback enabled.
105	Session timeout on the basis of encapsulation negotiations.
106	MP session timeout.
115	Instigating call no longer active.
120	Requested protocol is disabled or unsupported.
150	Disconnect requested by RADIUS server.
151	Call disconnected by local administrator.
152	Call disconnected via SNMP.
160	Exceeded maximum number of V.110 retries.
170	Timeout waiting to authenticate far end.
180	User disconnected by executing Do Hangup command from VT100 interface.
181	Call cleared by DSL Terminator.
185	Signal lost from far end, typically because the far end modem was turned off.
190	Resource has been deactivated.
195	Maximum duration time reached for call.
201	DSL Terminator has low memory.
210	DSL Terminator modem card stops working while it has calls outstanding.
220	DSL Terminator requires CBCP, but client does not support it.
230	DSL Terminator deleted Vrouter.
240	DSL Terminator disconnected call on the basis of LQM measurements.
241	DSL Terminator cleared backup call.
250	IP FAX call cleared normally.
251	IP FAX call cleared because of low available memory.
252	DSL Terminator detected an error for an incoming IP FAX call.
253	DSL Terminator detected an error for an outgoing IP FAX call.
254	DSL Terminator detected no available modem to support an IP FAX call.
255	DSL Terminator detected problem opening IP FAX session.
256	DSL Terminator detected a problem when performing a TCP function during an IP FAX call.
257	IP FAX session cleared abnormally.
258	DSL Terminator detected problem when parsing telephone number for IP FAX call.
260	DSL Terminator detected problem when decoding IP FAX variables.
261	DSL Terminator detected problem when decoding IP FAX variables.

Disconnect code	Description
262	DSL Terminator has no configured IP FAX server.

Following are the progress codes and their meanings:

Progress code	Description
1	Not applied to any call.
2	Unknown progress.
10	DSL Terminator has detected and accepted call.
30	DSL Terminator has assigned modem to call.
31	Modem is awaiting DCD from far-end modem.
32	Modem is awaiting result codes from far-end modem.
40	Terminal-server session started.
41	Raw TCP session started.
42	Immediate Telnet session started.
43	Connection made to raw TCP host.
44	Connection made to Telnet host.
45	Rlogin session started.
46	Connection made with Rlogin session.
47	Terminal-server authentication started.
50	Modem outdial session started.
60	LAN session is up.
61	Opening LCP.
62	Opening CCP.
63	Opening IPNCP.
64	Opening BNCP.
65	LCP opened.
66	CCP opened.
67	IPNCP opened.
68	BNCP opened.
69	LCP in Initial state.
70	LCP in Starting state.
71	LCP in Closed state.
72	LCP in Stopped state.
73	LCP in Closing state.
74	LCP in Stopping state.
75	LCP in Req-Sent state.
76	LCP in Ack-Rcvd state.
77	LCP in Ack-Sent state.

Progress code	Description
80	IPX NCP in Open state. (IPX is not applicable to DSL Terminator)
81	AT NCP in Open state.
82	BACP being opened.
83	BACP is now open.
84	CBCP being opened.
85	CBCP is now open.
90	DSL Terminator has accepted V.110 call.
91	V.110 call in Open state.
92	V.110 call in Carrier state.
93	V.110 call in Reset state.
94	V.110 call in Closed state.
100	DSL Terminator determines that call requires callback.
101	Authentication failed.
102	Remote authentication server timed out.
120	Frame Relay link is inactive. Negotiations are in progress.
121	Frame Relay link is active and has end-to-end connectivity.
200	Starting Authentication layer.
201	Authentication layer moving to opening state.
202	Skipping Authentication layer.
203	Authentication layer in opened state.

The backoff queue error message in the Syslog file

The DSL Terminator keeps accounting records until the accounting server acknowledges them. The backoff queue stores up to 100 unacknowledged records. If the unit never receives an acknowledgment to an accounting request, it eventually runs out of memory. To prevent this situation, the DSL Terminator might delete an accounting record and send the following error message to the Syslog file:

`Backoff Q full, discarding user` *`username`*

This error generally occurs for one of the following reasons:

- You enabled RADIUS accounting on the DSL Terminator but not on the RADIUS server.
- The Accounting Port or Accounting Key value is incorrect. The Accounting Key value must match the value assigned in the RADIUS clients file or in the TACACS+ configuration file.
- You are using the Livingston server instead of the Lucent server.

Syslog messages initiated by a SecureConnect Manger firewall

Depending on the settings specified in SecureConnect Manager (SCM), the DSL Terminator might generate Syslog messages about packets detected by a firewall. By default, SCM

specifies generation of a Syslog message about every packet blocked by the firewall. All messages initiated by a firewall are in the following format:

`date time router name ASCEND: interface message`

Element	Description
Date	The date the message was logged by Syslog
Time	The time the message was logged by Syslog.
Router name	The router this message was sent from.
Interface	The name of the interface (`ie0, wan0`, and so on) unless a call filter logs the packet as it brings up the link, in which case the word `call` appears.
Message	The message format has a number of fields, one or more of which may be present. See Table 5-8 for field definitions.

The message fields appear in the following order:

`protocol local direction remote length frag log tag`

Table 5-8. Syslog message fields for SecureConnect firewalls

Field	Description
`protocol`	The four-character (hexadecimal) Ether Type or one of the following network protocol names: ARP, RARP. For IP protocols, the field contains either the IP protocol number (up to three decimal digits) or one of the following names: IP-IN-IP, TCP, ICMP, UDP, ESP, AH. In the special case of ICMP, the field also includes the ICMP Code and Type ([*`Code`*]/[*`Type`*]/`icmp`).
`local`	For non-IP packets, *`local`* is the source Ethernet MAC address of transmitted packets and the destination Ethernet MAC address of received packets. For a nonbridged WAN connection, the two MAC addresses are all zeros. For IP protocols, *`local`* is the IP source address of transmitted packets and the IP destination address of received packets. In the case of TCP or UDP, it also includes the TCP or UDP port number ([*`IP-address`*];[*`port`*]).
`direction`	An arrow (<- or ->) indicating the direction in which the packet was traveling (receive and send, respectively).
`remote`	For non-IP protocols, *`remote`* has the same format that *`local`* has for non-IP packets, but shows the destination Ethernet MAC address of transmitted packets and the source Ethernet MAC address of received packets. For IP protocols, *`remote`* has the same format as *`local`* but shows the IP destination address of transmitted packets and the IP source address of received packets.
`length`	The length of the packet in octets (8-bit bytes).

Table 5-8. Syslog message fields for SecureConnect firewalls (continued)

Field	Description
frag	Indicates that the packet has a nonzero IP offset or that the IP More-Fragments bit is set in the IP header.
log	Reports one or more messages based on the packet status or packet header flags. The packet status messages include: • `corrupt`—the packet is internally inconsistent • `unreach`—the packet was generated by an "unreach=" rule in the firewall • `!pass`—the packet was blocked by the data firewall • `bringup`—the packet matches the call firewall • `!bringup`—the packet did not match the call firewall • `syn, fin, rst`—TCP flag bits. The `syn` bit is only displayed for the initial packet, which has the `syn` flag set instead of the `ack` flag set.
tag	Any user-defined tags specified in the filter template used by SCM

Sys Options window

The Sys Options window provides a read-only list that identifies your DSL Terminator and names each feature that has been installed. The following screen shows the Sys Options window:

```
00-100 Sys Options
>Security Prof:1   ^
 Software +1.0+
 S/N:42901
```

Table 5-9 describes the information that the Sys Options window can contain.

Table 5-9. Sys Options information

Option	Description
Security Prof: 1, Security Prof: 2...	Shows which of the nine Security profiles is active.
Software	Defines the version and revision of the system ROM code.
S/N	Displays the serial number of the DSL Terminator. The serial number of your DSL Terminator can also be found on the model number/serial number label on the DSL Terminator's bottom panel.
Up:*uptime*	Displays the system uptime in the following format: Up: *days*:*hours*:*minutes*:*seconds* For example: `Up: 13:12:18:26` The Days value *turns over* every 999 days. If the unit stays up continuously for 1000 days, the initial field resets to a 0 and begins incrementing again.
DSL Terminator	Identifies the DSL Terminator.
Load	Indicates the software load name. Lucent software releases are distributed in software loads, which vary according to the functionality and target platform for the binary.
Switched Installed or Switched Not Inst	Indicates whether the DSL Terminator can place calls over switched circuits.
Frm Rel Installed or Frm Rel Not Inst	Indicates whether the Frame Relay option is installed.
Sec Acc Installed or Sec Acc Not Installed	Indicates whether the Secure Connect Firewall option is installed.
Link Installed or Link Not Inst	Indicates whether the DSL Terminator Link option is installed.
PRI <-> T1 Installed or PRI <-> T1 Not Inst	Indicates whether the PRI to T1 signaling option is installed. The option is used for PBX support.
RS-366 Installed or RS-366 Not Inst	Indicates whether the EIA RS-366 dialing protocol has been installed.
Dyn Bnd Installed or Dyn Bnd Not Inst	Indicates whether Dynamic Bandwidth Allocation functionality is available.

Table 5-9. Sys Options information (continued)

Option	Description
AIM Nx56 Installed or AIM Nx56 Not Inst	Indicates whether Ascend Inverse Multiplexing (AIM) functionality is available. This functionality includes AIM remote management and BONDING, a prerequisite for Dynamic Bandwidth Allocation.
BONDING Installed or BONDING Not Inst	Indicates whether BONDING functionality is available.
V.25bis Installed or V.25bis Not Inst	Indicates whether the CCITT V.25 bis dialing and answering protocol is installed.
X.21 Installed or X.21 Not Inst	Indicates whether the X.21 dialing and answering protocol is installed.
Dial Installed or Dial Not Inst	Indicates whether the DSL Terminator Dial client software option is installed.
AuthServer: *a.b.c.d*	Shows the IP address of the current RADIUS authentication server for this unit.
AcctServer: *a.b.c.d*	Shows the IP address of the current RADIUS accounting server for this unit.
Dual Slot T1	Does not apply to this version of the DSL Terminator.
Data Call	Indicates whether the Hybrid Access option is installed.
SerialPortT1-CSU	Indicates whether the nailed T1 line is installed.

Note: Although GloBanD (Q.931W) does not appear in the Sys Options window, its presence can be verified by checking the value of the Switch Type parameter. For more information, see the *DSL Terminator Reference*.

System Status window

The System Status window is a branch of the Main Status Menu. It displays the windows that show the status of the DSL Terminator system as a whole.

The System Status window contains the following selections:

```
00-000 System
 00-100 Sys Options
>00-200 Message Log
 00-300 Port Info
 00-400 CDR
```

These selections provide information, about the DSL Terminator that pertains to the system as a whole and that would not fall under the classification of its T1 PRI line interfaces, its Ethernet interface, or its AIM host interface.

WAN Stat window

The WAN Stat window displays the current count of received frames, transmitted frames, and frames with errors for each active WAN link. It also indicates the overall count for all data packets received or transmitted across the WAN.

The following screen shows WAN statistics:

```
50-300 WAN Stat
>Rx Pkt:  387112
 Tx Pkt:   22092
    CRC:  0
```

The first line displays the window number and name of the window. You can press the Down-Arrow key to get per-link statistics. The first line of a per-link display shows the name, IP address, or MAC address of the remote device. The per-link count is updated every 30 seconds. The overall count is updated at the end of every active link.

The second and third lines show the number of frames received and transmitted, respectively. The fourth line indicates the number of CRC errors. A CRC error indicates a frame containing at least one data error.

Network Administration

6

Managing IP routes and sessions

This section describes how to monitor TCP/IP/UDP and related information using the terminal-server command-line interface. Using various IP route commands you can display and change the routing table, display routing statistics and display information about the operation of various routing protocols.

To invoke the terminal-server interface, select System > Sys Diag > Term Serv and press Enter. The terminal-server command-line prompt appears: `ascend%.`

Working with the IP routing table

The terminal-server IProute commands display the routing table and enable you to add or delete routes. The changes you make to the routing table by using the IProute command last only until the DSL Terminator is reset. To display the IProute commands, enter the IP route command with a question mark:

```
ascend% iproute ?
```

```
iproute ?       Display help information
iproute add     iproute add <destination/size> <gateway> [ pref ] [ m
iproute delete  iproute delete <destination/size> <gateway> [ proto ]
iproute show    displays IP routes (same as "show ip routes" command)
```

Displaying the routing table

You can use either the IProute Show command or the Show IP Routes command to display the IP routing table: For example:

```
ascend% iproute show
```

```
Destination        Gateway        IF       Flg Pref  Met   Use   Age
0.0.0.0/0          10.0.0.100     wan0     SG   1     1     0     20887
10.207.76.0/24     10.207.76.1    wanidle0 SG   100   7     0     20887
10.207.77.0/24     10.207.76.1    wanidle0 SG   100   8     0     20887
```

```
127.0.0.1/32        -              lo0      CP   0     0     0     20887
10.0.0.0/24         10.0.0.100     wan0     SG   100   1     21387 20887
10.1.2.0/24         -              ie0      C    0     0     19775 20887
10.1.2.1/32         -              lo0      CP   0     0     389   20887
255.255.255.255/32  -              ie0      CP   0     0     0     20887
```

The output includes the following information:

Field	Destination
`Destination`	Target address of a route. To send a packet to this address, the DSL Terminator uses this route. Note that the router uses the most specific route (having the longest mask) that matches a given destination.
`Gateway`	Address of the next hop router that can forward packets to the given destination. Direct routes (without a gateway) do not show a gateway address in the gateway column.
`IF`	Name of the interface through which a packet addressed to this destination is sent. • `ie0`—Ethernet interface • `lo0`— Loopback interface • `wanN`—Each of the active WAN interfaces • `wanidle0`— Inactive interface (the special interface for any route whose WAN connection is down).
`Flg`	Flag values. More than one flag value can be displayed. • `C`— A directly connected route, such as Ethernet • `I`—ICMP Redirect dynamic route • `N`—Placed in the table via SNMP MIB II • `R`—Route learned from RIP • `r`—RADIUS route • `S`—Static route • `?`—Route of unknown origin, which indicates an error • `G`—Indirect route via a gateway • `P`—Private route • `T`—Temporary route • `*`—Hidden route that will not be used unless another better route to the same destination goes down
`Pref`	Preference value of the route. Note that all routes that come from RIP have a preference value of 100, while the preference value of each individual static route can be set independently.
`Metric`	RIP-style metric for the route, with a valid range of 0-16. Routes learned from OSPF show a RIP metric of 10. OSPF Cost infinity routes show a RIP metric of 16.
`Use`	Count of the number of times the route was referenced since it was created. (Many of these references are internal, so this is not a count of the number of packets sent over this route.)

Field	Destination
`Age`	Age of the route in seconds, used for troubleshooting to determine when routes are changing rapidly or flapping.

Continuing the example, the first route shown is the default route with destination 0.0.0.0/0, defined through the active Connection profile.

```
0.0.0.0/0          10.0.0.100     wan0     SG   1     1     0     20887
```

The IP Route profile for the default route specifies a preference of 1, so this route is preferred over dynamically learned routes. The next route in this example, is specified in a Connection profile that is inactive (as indicated by the interface value wanidle0):

```
10.207.76.0/24     10.207.76.1    wanidle0 SG   100   7     0     20887
```

The next route in the table is a static route through an inactive gateway:

```
10.207.77.0/24     10.207.76.1    wanidle0 SG   100   8     0     20887
```

The static route is followed by the loopback route:

```
127.0.0.1/32       -              lo0      CP   0     0     0     20887
```

The loopback route specifies a special address. Packets sent to this special address are handled internally. The C flag indicates a connected route, while the P flag indicates that the router will not advertise this route.

The next route is specified in a Connection profile that is currently active:

```
10.0.0.0/24        10.0.0.100     wan0     SG   100   1     21387 20887
```

The first five routes followed by a connection to the Ethernet interface. It is directly connected, with a preference and metric of zero.

```
10.1.2.0/24        -              ie0      C    0     0     19775 20887
```

The last two routes are a private loopback route and a private route to the broadcast address:

```
10.1.2.1/32        -              lo0      CP   0     0     389   20887
255.255.255.255/32 -              ie0      CP   0     0     0     20887
```

The private loopback route shown is a host route with the Ethernet address. It is private, so it is not be advertised. The private route to the broadcast address is used in cases in which the router must to broadcast a packet, but the route is otherwise unconfigured. It is typically used when the DSL Terminator is trying to locate a server on a client machine to handle challenges for a token security card.

Adding an IP route

To add a static route that will be lost when the DSL Terminator resets enter the IProute Add command in the following format:

`iproute add` ***`destination gateway [metric]`***

where `destination` is the destination network address, ***`gateway`*** is the IP address of the router that can forward packets to that network, and ***`metric`*** is the virtual hop count to the destination network (default 8). For example, to add a route to the 10.1.2.0 network and all of

its subnets through the IP router located at 10.0.0.3/24 with a metric of 1 (the router is one hop away), enter the following command:

```
ascend% iproute add 10.1.2.0 10.0.0.3/24 1
```

If you try to add a route to a destination that already exists in the routing table, the DSL Terminator replaces the existing route, but only if it has a higher metric than the new route. If you get the message `Warning: a better route appears to exist`, the DSL Terminator has rejected your attempt to add a route because the routing table already contained a route, to the same destination, with a lower metric. Note that RIP updates can change the metric for the route.

Deleting an IP route

To remove a route from the DSL Terminator's routing table, enter the IProute Delete command in the following format:

```
iproute delete destination gateway
```

For example:

```
ascend% iproute delete 10.1.2.0 10.0.0.3/24
```

Note: RIP updates can add back any route you remove with IProute Delete. Also, after a system reset, the DSL Terminator restores all routes listed in the Static Route profile.

Displaying route statistics

The Traceroute command is useful for locating slow routers or diagnosing IP routing problems. It traces the route an IP packet follows by launching UDP probe packets with a low Time-To-Live (TTL) value and then listening for an ICMP time exceeded reply from a router. The Traceroute command uses the following syntax:

```
traceroute [-n] [-v] [-m max_ttl][-p port] [-q nqueries]
[-w waittime] host [datasize]
```

All flags are optional. The only required parameter is the destination hostname or IP address. The elements of the syntax are as follows:

Syntax element	**Description**
`-n`	Print hop addresses numerically rather than symbolically and numerically (this eliminates a name server address-to-name lookup for each gateway found on the path).
`-v`	Verbose output. Lists all received ICMP packets other than Time Exceeded and ICMP Port Unreachable are listed.
`-m max_ttl`	Sets the maximum time-to-live (maximum number of hops) for outgoing probe packets. The default is 30 hops.
`-p port`	Set the base UDP port number used in probes. Traceroute depends on having nothing listening on any of the UDP ports from the source to the destination host (so that an ICMP Port Unreachable message will be returned to terminate the route tracing). If something is listening on a port in the default range, you can set the `-p` option to specify an unused port range. The default is 33434.

`-q nqueries`	Set the maximum number of queries for each hop. The default is 3.
`-w waittime`	Set the time to wait for a response to a query. The default is 3 seconds.
`host`	The destination host by name or IP address.
`datasize`	Sets the size of the data field of the UDP probe datagram sent by Traceroute. The default is 0. This results in a datagram size of 38 bytes (a UDP packet carrying no data).

For example, to trace the route to the host `techpubs`:

```
ascend% traceroute techpubs

traceroute to techpubs (10.65.212.19), 30 hops, 0 byte packets
 1  techpubs.eng.ascend.com (10.65.212.19)  0 ms  0 ms  0 ms
```

Probes start with a TTL of 1 and increase by one until one of the following conditions occurs:

- The DSL Terminator receives an ICMP Port Unreachable message.

  The UDP port in the probe packets is set to an unlikely value, such as 33434, because the target host is not intended to process the packets. A “port unreachable” message indicates that the packets reached the target host and were rejected.
- The TTL value reaches the maximum value.

  By default, the maximum TTL is set to 30. You can specify a different TTL by using the `–m` option. For example:

```
ascend% traceroute -m 60 techpubs

traceroute to techpubs (10.65.212.19), 60 hops, 0 byte packets
 1  techpubs.eng.abc.com (10.65.212.19)  0 ms  0 ms  0 ms
```

Three probes are sent at each TTL setting. The second line of command output shows the address of the router and round-trip time of each probe. If the probe answers come from different gateways, the address of each responding system is shown. If there is no response within a 3 second time-out interval, the command output is an asterisk. The following annotations can appear after the time field in a response:

- `!H`—Host reached.
- `!N`—Network unreachable.
- `!P`—Protocol unreachable.
- `!S`—Source route failed. Might indicate a problem with the associated device.
- `!F`—Fragmentation needed. Might indicate a problem with the associated device.
- `!h`—Communication with the host is prohibited by filtering.
- `!n`—Communication with the network is prohibited by filtering.
- `!c`—Communication is otherwise prohibited by filtering.
- `!?`—ICMP subcode detected. This event should not occur.
- `!??`—Reply received with inappropriate type. This event should not occur.

Pinging other IP hosts

The terminal-server Ping command is useful for verifying that the transmission path is open between the DSL Terminator and another station. It sends an ICMP echo-request packet to the

specified station. If the station receives the packet, it returns an ICMP echo-response packet. The Ping command has the following syntax:

```
ping [-q] [-v] [-c count] [-i sec | -I msec] [-s packetsize]
[-x src_address] host
```

All flags are optional. The only required parameter is the destination hostname or IP address. The elements of the syntax are as follows:

Syntax element	Description
`-q`	Quiet mode. The DSL Terminator displays only the summary of all Ping responses it has received.
`-v`	Verbose output. The DSL Terminator displays information from each ping response that it receives as well as the summary of all Ping responses. This is the default.
`-c` *`count`*	Specifies the number of Ping requests that the DSL Terminator sends to the host. By default, the DSL Terminator sends continual Ping requests until you press Ctrl-C.
`-i` *`sec`*	Specifies the length of time, in seconds, between Ping requests. You can specify seconds, using the `-i` option, or milliseconds, using the `-I` option, but not both. The default is one second.
`-I` *`msec`*	Specifies the length of time, in milliseconds, between Ping requests. You can specify milliseconds, using the `-I` option, or seconds, using the `-i` option, but not both.
`-s` *`packetsize`*	Specifies the size of each Ping request packet that the DSL Terminator sends to the host. The default is 64 bytes.
`-x` *`srcaddress`*	Specifies a source IP address that overwrites the default source address.
`host`	The destination host by name or IP address.

For example, to Ping the host `techpubs`:

```
ascend% ping techpubs

PING techpubs (10.65.212.19): 56 data bytes
64 bytes from 10.65.212.19: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 10.65.212.19: icmp_seq=3 ttl=255 time=0 ms
^C
--- techpubs ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/DSL MAX= 0/0/0 ms
```

You can terminate the Ping exchange at any time by pressing Ctrl-C. When you press Ctrl-C, the command reports the number of packets sent and received, the percentage of packet loss, any duplicate or damaged echo-response packets, and round-trip statistics. In some cases, round-trip times cannot be calculated.

During the Ping exchange, the DSL Terminator displays information about the packet exchange, including the Time-To-Live (TTL) of each ICMP echo-response packet.

Note: Because the maximum TTL for ICMP Ping is 255 and the maximum TTL for TCP is often 60 or lower, you might be able to Ping a host but be unable to run a TCP application (such as Telnet or FTP) to that station. If you Ping a host running a version of Berkeley UNIX earlier than 4.3BSD-Tahoe, the TTL report is 255 minus the number of routers in the round-trip path. If you Ping a host running the current version of Berkeley UNIX, the TTL report is 255 minus the number of routers in the path from the remote system to the station performing the Ping.

The Ping command sends an ICMP mandatory echo-request datagram, which asks the remote station “Are you there?” If the echo-request reaches the remote station, the station sends back an ICMP echo-response datagram, which tells the sender “Yes, I am alive.” This exchange verifies that the transmission path is open between the DSL Terminator and a remote station.

Configuring the DNS fallback table

The local DNS table provides a list of IP addresses for a specific host name when the remote DNS server fails to resolve the host name. If the local DNS table contains the host name for the attempted connection, it provides the list of IP addresses.

You create the DNS table from the Ethernet > Mod Config > DNS menu by entering up to eight host names. Enter the IP addresses for each host through the terminal-server interface. You can configure a maximum of 35 IP addresses for each host. If you specify automatic updating, you only have to enter the first IP address of each host. Additional IP addresses are added automatically.

Automatic updating replaces the existing address list for a host each time the remote DNS server succeeds in resolving a connection to a host that is in the table. You specify how many of the addresses returned by the remote server can be included in the new list.

On the DSL Terminator, the table, which you display from the terminal-server interface, provides additional information for each table entry. The information is in the following two fields, which are updated when the system matches the table entry with a host name that was not found by the remote server:

- # Reads (the number of reads since entry was created). This field is updated each time a local name query match is found in the local DNS table.
- Time of Last Read

You can use the terminal-server command Show Dnstab to check the list of host names and IP addresses in the table. Figure 6-1 shows an example of a DNS table on a DSL Terminator.

Figure 6-1. Example of a local DNS table

```
Local DNS Table
Name                      IP Address      # Reads Time of last read
_________________________ _______________ _______ ___________________
1: ""                     ------          ------
2: "server.corp.com."     200.0.0.0       2       Feb 10 10:40:44
3: "boomerang"            221.0.0.0       2       Feb 10  9:13:33
4: ""                     ------          -------
5: ""                     ------          -------
6  ""                     ------          -------
7: ""                     ------          -------
```

Displaying IP routing and related information

The following Show commands for monitoring IP routing and related protocols are described in this section:

```
show arp         Display the Arp Cache
show icmp        Display ICMP information
show if          Display Interface info. Type 'show if ?' for help.
show ip          Display IP information. Type 'show ip ?' for help.
show udp         Display UDP information. Type 'show udp ?' for help.
show tcp         Display TCP information. Type 'show tcp ?' for help.
show pools       Display the assign address pools.
```

Displaying the ARP cache

To display the ARP cache, enter the Show ARP command. For example:

```
ascend% show arp

entry typ ip address      ether addr    if rtr pkt   insert
    0 DYN 10.65.212.199  00C07B605C07   0   0   0   857783
    1 DYN 10.65.212.91   0080C7C4CB80   0   0   0   857866
    2 DYN 10.65.212.22   080020792B4C   0   0   0   857937
    3 DYN 10.65.212.3    0000813DF048   0   0   0   857566
    4 DYN 10.65.212.250  0020AFF80F1D   0   0   0   857883
    5 DYN 10.65.212.16   0020AFEC0AFB   0   0   0   857861
    6 DYN 10.65.212.227  00C07B5F14B6   0   0   0   857479
    7 DYN 10.65.212.36   00C07B5E9AA5   0   0   0   857602
    8 DYN 10.65.212.71   0080C730041F   0   0   0   857721
    9 DYN 10.65.212.5    0003C6010512   0   0   0   857602
   10 DYN 10.65.212.241  0080C72ED212   0   0   0   857781
   11 DYN 10.65.212.120  0080C7152582   0   0   0   857604
   12 DYN 10.65.212.156  0080A30ECE6D   0   0   0   857901
   13 DYN 10.65.212.100  00C07B60E28D   0   0   0   857934
   14 DYN 10.65.212.1    00000C065D27   0   0   0   857854
   15 DYN 10.65.212.102  08000716C449   0   0   0   857724
```

```
16 DYN 10.65.212.33   00A024AA0283   0   0   0   857699
17 DYN 10.65.212.96   0080C7301792   0   0   0   857757
18 DYN 10.65.212.121  0080C79BF681   0   0   0   857848
19 DYN 10.65.212.89   00A024A9FB99   0   0   0   857790
20 DYN 10.65.212.26   00A024A8122C   0   0   0   857861
21 DYN 10.65.212.6    0800207956A2   0   0   0   857918
22 DYN 10.65.212.191  0080C75BE778   0   0   0   857918
23 DYN 10.65.212.116  0080C72F66CC   0   0   0   857416
24 DYN 10.65.212.87   0000813606A0   0   0   0   857666
25 DYN 10.65.212.235  00C07B76D119   0   0   0   857708
26 DYN 10.65.212.19   08002075806B   0   0   0   857929
```

The ARP table displays the following information:

Field	Description
Entry	A unique identifier for each ARP table entry.
Typ	How the address was learned, dynamically (DYN) or statically (STAT)
IP Address	The address contained in ARP requests.
Ether Addr	The MAC address of the host with that IP address.
IF	The interface on which the DSL Terminator received the ARP request.
RTR	The next-hop router on the specified interface.

Displaying ICMP packet statistics

To display the number of ICMP packets received intact, received with errors, and transmitted, enter the Show Icmp command. For example:

```
ascend% show icmp

3857661 packet received.
20 packets received with errors.
   Input histogram: 15070
2758129 packets transmitted.
0 packets transmitted due to lack of resources.
   Output histogram: 15218
```

The Input and Output histograms show the number of ICMP packets received and transmitted, respectively.

Displaying interface statistics

To display the supported interface-statistics commands, enter the Show if command with a question mark. For example:

```
ascend% show if ?
```

```
show if ?                 Display help information
show if stats             Display Interface Statistics
show if totals            Display Interface Total counts
```

To display the status and packet count of each active WAN link and of local and loopback interfaces, enter the Show if stats command. For example:

```
ascend% show if stats
Interface    Name    Status  Type     Speed    MTU   InPackets    Out-
packet
ie0        ethernet    Up    6     10000000   1500     107385     85384
wan0                 Down    1            0   1500       0          0
wan1                 Down    1            0   1500       0          0
wan2                 Down    1            0   1500       0          0
wanidle0               Up    6     10000000   1500       0          0
lo0       loopback     Up   24     10000000   1500       0          0
```

The output contains the following fields:

Field	Description
Interface	Interface name. For more information, see the *Network Configuration Guide* for your DSL Terminator.
Name	Name of the profile or a text name for the interface.
Status	Up (the interface is functional) or Down (the interface is not functional).
Type	Type of application being used on the interface, as specified in RFC 1213 (MIB-2). For example, 23 indicates PPP.
Speed	Data rate in bits per second.
MTU	The maximum packet size allowed on the interface. MTU stands for Maximum Transmission Unit.
InPackets	The number of packets the interface has received.
OutPackets	The number of packets the interface has transmitted.

To display the packet count at each interface, broken down by type of packet, enter the Show If Totals command. For example:

```
ascend% show if totals
Name  --Octets----Ucast-- -NonUcast- Discard -Error- Unknown -Same IF-
ie0  i:   7813606   85121     22383       0        0       0        0
     o: 101529978   85306       149       0        0       0        0
wan0 i:         0       0         0       0        0       0        0
     o:         0       0         0       0        0       0        0
wan1 i:         0       0         0       0        0       0        0
     o:         0       0         0       0        0       0        0
wan2 i:         0       0         0       0        0       0        0
     o:         0       0         0       0        0       0        0
wanidle0 i:     0       0         0       0        0       0        0
         o:     0       0         0       0        0       0        0
lo0  i:         0       0         0       0        0       0        0
     o:         0       0         0       0        0       0        0
```

The output contains the following fields:

Field	Description
`Name`	Interface name. For more information, see the *`Network Configuration Guide`* for your DSL Terminator.
`Octets`	Total number of bytes processed by the interface.
`Ucast`	Packets with a unicast destination address.
`NonUcast`	Packets with a multicast address or a broadcast address.
`Discard`	Number of packets that the interface could not process.
`Error`	Number of packets with CRC errors, header errors, or collisions.
`Unknown`	Number of packets the DSL Terminator forwarded across all bridged interfaces because of unknown or unlearned destinations.
`Same if`	Number of bridged packets whose destination is the same as the source.

Displaying IP statistics and addresses

To display the IP statistics and addresses supported commands, enter the Show IP command with a question mark:

```
ascend% show ip ?
```

```
show ip ?           Display help information
show ip stats       Display IP Statistics
show ip address     Display IP Address Assignments
show ip routes      Display IP Routes
```

Note: For information about the Show IP Routes command, see “Working with the IP routing table” on page 6-1.

To display statistics on IP activity, including the number of IP packets the DSL Terminator has received and transmitted, enter the Show IP Stats command. For example:

```
ascend% show ip stats
```

```
107408 packets received.
     0 packets received with header errors.
     0 packets received with address errors.
     0 packets forwarded.
     0 packets received with unknown protocols.
     0 inbound packets discarded.
107408 packets delivered to upper layers.
 85421 transmit requests.
     0 discarded transmit packets.
     1 outbound packets with no route.
     0 reassembly timeouts.
     0 reassemblies required.
     0 reassemblies that went OK.
     0 reassemblies that Failed.
     0 packets fragmented OK.
     0 fragmentations that failed.
     0 fragment packets created.
```

```
    0 route discards due to lack of memory.
    64 default ttl.
```

To display IP interface address information, enter the Show IP Address command. For example:

```
ascend% show ip address

Interface   IP Address    Dest Address   Netmask         MTU     Status
ie0         10.2.3.4      N/A            255.255.255.224   1500      Up
wan0        0.0.0.0       N/A            0.0.0.0           1500    Down
wan1        13.1.2.0      13.1.2.128     255.255.255.248   1500    Down
wan2        0.0.0.0       N/A            0.0.0.0           1500    Down
wan3        0.0.0.0       N/A            0.0.0.0           1500    Down
lo0         127.0.0.1     N/A            255.255.255.255   1500      Up
rj0         127.0.0.2     N/A            255.255.255.255   1500      Up
bh0         127.0.0.3     N/A            255.255.255.255   1500      Up
```

Displaying UDP statistics and listen table

To display the supported UDP-statistics commands, enter the Show UDP command with a question mark:

```
ascend% show udp ?

show udp ?          Display help information
show udp stats      Display UDP Statistics
show udp listen     Display UDP Listen Table
```

To display the number of UDP packets received and transmitted, enter the Show UDP Stats command. For example:

```
ascend% show udp stats

22386 packets received.
    0 packets received with no ports.
    0 packets received with errors.
    0 packets dropped
    9 packets transmitted.
```

The Show Udp Listen command displays the socket number, UDP port number and the number of packets queued for each UDP port on which the DSL Terminator is currently listening.

For example:

```
ascend% show udp listen

udp:
Socket Local Port InQLen InQMax    InQDrops    Total Rx
0         1023      0       1           0           0
1         520       0       50          0           532
2         7         0       32          0           0
3         123       0       32          0           0
4         1022      0       128         0           0
5         161       0       64          0           0
```

The command's output also includes the following fields:

Field	Description
`InQMax`	Maximum number of queued UDP packets on the socket. (See Queue Depth and Rip Queue Depth parameters.)
`InQLen`	Current number of queued packets on the socket.
`InQDrops`	Number of packets discarded because it would cause InQLen to exceed InQMax.
`Total Rx`	Total number of packets received on the socket, including InQDrops.

Displaying TCP statistics and connections

To display the supported TCP-statistics commands, enter the Show TCP command with a question mark:

```
ascend% show tcp ?

show tcp ?          Display help information
show tcp stats      Display TCP Statistics
show tcp connection Display TCP Connection Table
```

To display the number of TCP packets received and transmitted, enter the Show TCP Stats command. For example:

```
ascend% show tcp stats

     0 active opens.
    11 passive opens.
     1 connect attempts failed.
     1 connections were reset.
     3 connections currently established.
 85262 segments received.
 85598 segments transmitted.
   559 segments re-transmitted.
```

An active open is a TCP session that the DSL Terminator initiated, and a passive open is a TCP session that the DSL Terminator did not initiate.

To display current TCP sessions:

```
ascend% show tcp connection

Socket       Local              Remote                        State
0            *.23               *.*                         LISTEN
1            10.2.3.23          15.5.248.121.15003      ESTABLISHED
```

Displaying address pool status

To view the status of the DSL Terminator's IP address pool:

```
ascend% show pools

Pool #         Base        Count             InUse
1              10.98.1.2     55              27
2              10.5.6.1     128              0
   Number of remaining allocated addresses: 0
```

If you change an address pool while users are still logged in using the addresses from the previous pool, `Number of remaining allocated addresses` reflects how many users are currently using addresses from the previous pool. Typically, the value is 0 (zero).

Managing multicast routing

The terminal-server command-line interface provides commands to support IP multicast functionality. To display the options, invoke the terminal-server interface (System > Sys Diag > Term Serv) and enter the Show IGMP and/or show Mrouting command with a question mark:

```
ascend% show igmp ?

show igmp ?                Display help information
show igmp stats            Display IGMP Statistics
show igmp groups           Display IGMP groups Table
show igmp clients          Display IGMP clients

ascend% show mrouting ?

show mrouting ?        Display help information
show mrouting stats    Display MROUTING Statistics
```

Displaying the multicast forwarding table

To display active multicast group addresses and clients (interfaces) registered for each group:

```
ascend% show igmp groups

IGMP Group address Routing Table Up Time: 0:0:22:17
Hash      Group Address    Members    Expire time   Counts
N/A      Default route      *(Mbone)    ......     2224862
10       224.0.2.250
                             2           0:3:24       3211 :: 0 S5
                             1           0:3:21       145 :: 0 S5
                             0(Mbone)    ......       31901 :: 0 S5
```

The output includes the following fields:

Field	Description
`Hash`	Index to a hash table that is displayed for debugging purposes only. The Default route is not an entry in the hash table.
`Group Address`	IP multicast address used. The Default route is the interface on which the multicast router resides. **Note:** If the IP multicast address being monitored is marked with an asterisk, it means that this address is joined by local application.
`Members`	Interface ID on which the membership resides. The number 0 represents the Ethernet interface. Other numbers represent WAN interfaces, numbered according to when they became active. The interface labeled `Mbone` is the one on which the multicast router resides.

Field	Description
`Expire time`	Time at which this membership expires. The DSL Terminator sends out IGMP queries every 60 seconds, so the expiration time is usually renewed. If the expiration time is reached, the entry is removed from the table. Periods in this field indicates that the membership never expires.
`Counts`	Number of packets forwarded to the client, number of packets dropped because of a lack of resources, and state of the membership (the state is displayed for debugging purposes).

Listing multicast clients

To display a list of multicast clients, enter the Show igmp Clients command. For example:

```
ascend% show igmp clients
IGMP Clients

Client      Version  RecvCount  CLU      ALU
  0(Mbone)      1       0          0       0
  2             1      39         68       67
  1             1   33310         65       65
```

The output includes the following fields:

Field	Description
`Client`	Interface ID on which the client resides. The number 0 represents the Ethernet. Other numbers are WAN interfaces, numbered in the order they became active. The interface labeled `Mbone` is the one on which the multicast router resides.
`Version`	Version of IGMP being used.
`RecvCount`	Number of IGMP messages received on that interface.
`CLU` (Current Line Utilization) and `ALU` (Average Line Utilization)	Percentage of bandwidth utilized across this interface. If bandwidth utilization is high, some IGMP packet types will not be forwarded.

Displaying multicast activity

To display the number of IGMP packet types sent and received, enter the Show igmp Stats command. For example:

```
ascend% show igmp stats
       46 packets received.
        0 bad checksum packets received.
        0 bad version packets received.
        0 query packets received.
       46 response packets received.
        0 leave packets received.
```

```
       51 packets transmitted.
       47 query packets sent.
        4 response packets sent.
        0 leave packets sent.
```

To display the number of multicast packets received and forwarded, enter the Show Mrouting Stats commands. For example:

```
ascend% show mrouting stats

34988 packets received.
    57040 packets forwarded.
        0 packets in error.
       91 packets dropped.
        0 packets transmitted.
```

In many cases, the number of packets forwarded is greater than the number of packets received, because packets can be duplicated and forwarded across multiple links.

Managing virtual routing

Terminal server commands can be used to obtain information about virtual routing.

Terminal Server commands

The following commands support virtual routing. If you do not specify a VRouter name on the command line, the DSL Terminator unit applies the command to global VRouter settings. If you specify a VRouter name, the DSL Terminator unit applies the command to the specified VRouter.

Command	Syntax with optional VRouter arguments
IProute	`iproute add [-r vRouterName] destination/size [gateway] [pref][metric][proto]`
	`iproute delete [-r vRouterName] destination/size [gateway]`
Traceroute	`traceroute [-n] [-v] [-m max_ttl] [-p port] [-q nqueries] [-w waittime] [-r vRouter] [-s src_addr] host-name [datasize]`
Ping	`ping [-q | -v] [-i sec | -I msec] [-s packet-size] [-r vRouter] [-x source_address] host-name`
Telnet	`telnet [-a | -b | -t] [-v VRouterName] [-l[e] | -r[e]] host-name [port-number]`

The following Show commands support virtual routing. If you do not specify a VRouter name on the terminal server command line, the DSL Terminator unit displays global VRouter information. If you specify a VRouter name, the DSL Terminator unit displays information about the specified VRouter.

Command	Syntax with optional VRouter arguments
IPRoutes	`show iproutes [-r vrouterName] [dest]`

Command	Syntax with optional VRouter arguments
IPStats	`show ip stats [[-r] vrouterName]`
IPaddress	`show ip address [[-r] vrouterName] [all]`
ICMP	`show icmp [[-r] vrouterName]`
UDP	`show udp stats [[-r] vrouterName]`
	`show udp listen [[-r] vrouterName]`
TCP	`show tcp stats [[-r] vrouterName]`
	`show tcp connection [[-r] vrouterName]`
Pools	`show pools [[-r] vrouterName]`

Monitoring Frame Relay connections

The terminal-server command-line interface includes Show fr commands for monitoring Frame Relay in the DSL Terminator. To display the options, invoke the terminal-server interface (System > Sys Diag > Term Serv) and enter the Show fr command with a question mark:

```
ascend% show fr ?

show fr ?Display help information
show fr statsDisplay Frame Relay information
show fr lmiDisplay Frame Relay LMI information
show fr dlci [name]Display all DLCI information or just for [name]
show fr circuitsDisplay the FR Circuit table
```

Displaying Frame Relay statistics

To display Frame Relay statistics, enter the Show fr Stats commands: For example:

```
ascend% show fr stats

Name         Type   Status    Speed    MTU     InFrame     OutFrame
fr1          DCE    Down     64000    1532           0            1
fr1-temp     DCE      Up     64000    1532           0            1
fr1-temp-9   DCE      Up     64000     1532          0            0
```

The output includes the following fields:

Field	Description
`Name`	Name of the Frame Relay profile associated with the interface.
`Type`	Type of interface.
`Status`	Status of the interface. Up means the interface is functional, but is not necessarily handling an active call. Down means the interface is not functional.
`Speed`	Data rate in bits per second.
`MTU`	Maximum packet size allowed on the interface.

Field	Description
InFrame	Number of frames the interface has received.
OutFrame	Number of frames transmitted.

Displaying link management information

To display Link Management Information (LMI) for each link activated by a Frame Relay profile, enter the Show fr lmi command. For example:

```
ascend% show fr lmi

T1_617D LMI for fr1
  Invalid Unnumbered info         0  Invalid Prot Disc               0
  Invalid Dummy Call Ref          0  Invalid Msg Type                0
  Invalid Status Message          0  Invalid Lock Shift              0
  Invalid Information ID          0  Invalid Report Type             0
  Num Status Enqs Sent            0  Num Status Msgs Rcvd            0
  Num Update Status Rcvd          0  Num Status Timeouts          2779

LMI is not on for fr1-temp
LMI is not on for fr1-temp-9
```

ANSI T1.617 Annex D local in-channel signaling protocol is the basis for this information. (For a full definition of each of the fields reported, see Annex D.)

Displaying Data Link Connection Indicator (DLCI)status

To display the status of each Data Link Connection Indicator (DLCI), enter the Show fr lmi command. For example:

```
ascend% show fr dlci

DLCIs for fr1

DLCIs for fr1-temp

eng-lab-236-CirDLCI =   17Status = ACTIVE

       input pkts0output pkts0
       input octets0output octets0
       input FECN0input DE0
       input BECN0
last time status changed: 03/05/1997  14:44:17

DLCIs for fr1-temp-9

eng-lab-236-Cir-9  DLCI =   16    Status = ACTIVE
       input pkts0output pkts0
       input octets0output octets0
       input FECN0input DE0
       input BECN0
last time status changed: 03/05/1997  14:45:07

DLCIs not assigned
```

The output includes the following fields:

Field	Description
DLCI	DLCI number.
Status	ACTIVE if the connection is up or INACTIVE if not.
input pkts	Number of frames the interface has received.
output pkts	Number of frames the interface has transmitted.
input octets	Number of bytes the interface has received.
output octets	Number of bytes the interface has transmitted.
in FECN pkts	Number of packets received with the Forward Explicit Congestion Notification (FECN) bit set. This field always contains a 0 (zero), because congestion management is not currently supported.
in BECN pkts	Number of packets received with the Backward Explicit Congestion Notification (BECN) bit set. This field always contains a 0 (zero), because congestion management is not currently supported.
in DE pkts	Number of packets received with the Discard Eligibility (DE) indicator bit set.
last time status changed	Time at which the DLCI state changed.

Displaying circuit information

The Show fr Circuits command displays the Frame Relay profile name, the DLCI, and the status of configured circuits. For example:

```
ascend% show fr circuits

cir-9 User Setting Up
fr1-temp-916 Up
fr1-temp17   Up
```

Turning off a circuit without disabling its endpoints

The Set Circuit command enables you to turn off traffic going through a Frame Relay circuit without disabling the circuit endpoints. This command prevents traffic from traveling between endpoints, but does not disrupt the state of the DLCI. To display the support options:

```
ascend% set circuit ?

set circuit ?       Display help information
set circuit active [name]  Set the CIRCUIT to active
set circuit inactive [name]  Set the CIRCUIT to inactive
```

To allow data to flow through a circuit, enter the Set Circuit Active command and append the name of the circuit. parameter. For example:

```
ascend% set circuit active circuit-1
```

To turn off data flow without disrupting the state of the DLCIs, enter the Set Circuit Inactive command and append the name of the circuit. For example:

```
ascend% set circuit inactive circuit-2
```

SNMP and Syslog Configuration 7

DSL Terminator configurations control which classes of events will generate traps to be sent to an SNMP manager, and which managers have SNMP access to the unit. A configuration includes community strings to prevent unauthorized access. This chapter shows you how to set up the unit to work with SNMP.

Configuring SNMP

The DSL Terminator supports Simple Network Management Tool (SNMP) on a TCP/IP network. An SNMP management station that uses the Ascend Enterprise MIB can query the DSL Terminator, set some parameters, sound alarms when certain conditions appear in the DSL Terminator, and so forth. An SNMP manager must be running on a host on the local IP network, and the DSL Terminator must be able to find that host, through either a static route or RIP.

The DSL Terminator supports the Ascend Enterprise MIB, MIB II, and some ancillary SNMP features. The DSL Terminator can send management information to an SNMP manager without being polled. SNMP security uses a community name sent with each request. The DSL Terminator supports two community names, one with read-only access, and the other with read/write access to the MIB.

SNMP has its own password security. Lucent recommends that you set up SNMP password security to prevent reconfiguration of the DSL Terminator from an SNMP station.

Configuring SNMP access security

There are two levels of SNMP security: community strings, which must be known by a community of SNMP managers to access the box, and address security, which excludes SNMP access unless it is initiated from a specified IP address. Following are the relevant parameters (shown with sample settings):

```
Ethernet
   Mod Config
      SNMP options...
         Read Comm=Ascend
         R/W Comm Enable=No
```

```
R/W Comm=Secret
Security=Yes
RD Mgr1=10.0.0.1
RD Mgr2=10.0.0.2
RD Mgr3=10.0.0.3
RD Mgr4=10.0.0.4
RD Mgr5=10.0.0.5
WR Mgr1=10.0.0.11
WR Mgr2=10.0.0.12
WR Mgr3=10.0.0.13
WR Mgr4=10.0.0.14
WR Mgr5=10.0.0.15
```

For complete information about each parameter, see the *DSL Terminator Reference*.

Enabling SNMP Set commands

The R/W Comm Enable parameter disables SNMP set commands by default. Before you can use an SNMP Set command, you must set R/W Comm Enable to `Yes`.

Note: Even if you enable R/W Comm, you must still know the read-write community string to use a Set command.

Setting community strings

The Read Comm parameter specifies the SNMP community name for read access (up to 32 characters), and the R/W Comm parameter specifies the SNMP community name for read/write access.

Setting up and enforcing address security

If the Security parameter is set to `No` (its default value), any SNMP manager that presents the right community name will be allowed access. If you set this parameter to Yes, the DSL Terminator checks the source IP address of the SNMP manager and allows access only to those IP addresses listed in the RD Mgr*N* and WR Mgr*N* parameters, each of which specifies up to five host addresses.

Resetting and verifying reset

You can use SNMP (`sysReset` object) to reset a DSL Terminator from an SNMP manager. After the Reset command is issued, a one-minute time-out (not modifiable) permits the DSL Terminator to confirm the request before the unit is reset.

Information held in the Ascend Events Group is erased and its values are initialized when the DSL Terminator is reset by software or by toggling the power off and on. The SNMP object `sysAbsoluteStartupTime` is the time in seconds since January 1, 1990, and is not modified. To determine whether the DSL Terminator has actually reset, you can retrieve `sysAbsoluteStartupTime` and compare its value against the previous poll's value for Ascend Events Group variables.

Example of SNMP security configuration

The following procedure sets the community strings, enforces address security, and prevents write access:

1. Open Ethernet > Mod Config > SNMP Options.
2. Set R/W Comm Enable to `Yes`.
3. Specify the Read Comm and R/W Comm parameter strings.
4. Set Security to `Yes`.
5. Specify up to five host addresses in the RD Mgr*N* parameters. Leave the WR Mgr*N* parameters set to zero to prevent write access.
6. Close the Ethernet profile.

Following is an example of a profile configured with the preceding procedure.

```
Ethernet
   Mod Config
      SNMP options...
         Read Comm=Secret-1
         R/W Comm Enable=Yes
         R/W Comm=Secret-2
         Security=Yes
         RD Mgr1=10.0.0.1
         RD Mgr2=10.0.0.2
         RD Mgr3=10.0.0.3
         RD Mgr4=10.0.0.4
         RD Mgr5=10.0.0.5
         WR Mgr1=0.0.0.0
         WR Mgr2=0.0.0.0
         WR Mgr3=0.0.0.0
         WR Mgr4=0.0.0.0
         WR Mgr5=0.0.0.0
```

Setting SNMP traps

A trap is a mechanism for reporting system change in real time (for example, reporting an incoming call to a serial host port). When a trap is generated by some condition, a traps-PDU (Protocol Data Unit) is sent across the Ethernet to the SNMP manager.

Following are the parameters related to setting SNMP traps (shown with sample settings):

```
Ethernet
   SNMP Traps
      Name=
      Alarm=Yes
      Port=Yes
      Security=Yes
      Comm=
      Dest=10.2.3.4
```

For complete information about each parameter and the events that generate traps in the various classes, see the *DSL Terminator Reference*.

Understanding the SNMP trap parameters

To specify the SNMP trap profile name, set the Name parameter. Use a name of 31 or fewer characters.

To specify the community string for communicating with the SNMP manager, set the Comm parameter to the community name associated with the SNMP PDU.

The Alarm, Port, and Security fields specify whether the DSL Terminator traps respectively alarm events, port events, and/or security events, and sends a trap-PDU to the SNMP manager.

The Dest field specifies the destination address for the trap-status report. If DNS or YP/NIS is supported, the Dest field can contain the hostname of a system running an SNMP manager. If the DNS or YP/NIS is not supported, the Dest field must contain the host's address.

Note: To turn off SNMP traps, set Dest to 0.0.0.0 and delete the value for Comm.

Example SNMP trap configuration

The following procedure creates a profile that specifies a community name, all the trap types, and the host's IP address in the Dest parameter.

1. Open an SNMP Traps profile and assign it a name.
2. Specify the community name (for example, Ascend).
3. Set the trap types to `Yes`.
4. Specify the IP address of the host to which the trap-PDUs will be sent.
5. Close the SNMP Traps profile.

Following is an example of a profile configured with this procedure:

```
Ethernet
   SNMP Traps
      Name=security-traps
      Alarm=Yes
      Port=Yes
      Security=Yes
      Comm=Ascend
      Dest=10.2.3.4
```

Ascend enterprise traps

This section provides a brief summary of the traps generated by alarm, port, and security events. For more details, see the Ascend Enterprise MIB. To obtain the Ascend MIB, see "Supported MIBs" on page 7-7.

Alarm events

Alarm events (also called *error events*) use trap types defined in RFC 1215 and RFC 1315, as well as an Ascend enterprise trap type. The DSL Terminator provides the following trap types:

Alarm event	Signifies that the DSL Terminator sending the trap
coldStart (RFC-1215 trap-type 0)	Is reinitializing itself and that the configuration of the SNMP manager or the unit might be altered.
warmStart (RFC-1215 trap-type 1)	Is reinitializing itself but neither the configuration of the SNMP manager nor that of the unit will be altered.
linkDown (RFC-1215 trap-type 2)	Recognizes a failure in one of the communication links represented in the SNMP manager's configuration.
linkUp (RFC-1215 trap-type 3)	Recognizes that one of the communication links represented in the SNMP manager's configuration has come up.
frDLCIStatusChange (RFC-1315 trap-type 1)	Recognizes that one of the virtual circuits (to which a DLCI number has been assigned) has changed state. That is, the link has either been created or invalidated, or has toggled between the active and inactive states.
eventTableOverwrite (ascend trap-type 16)	Detects that a new event has overwritten an unread event. This trap is sent only for systems that support Ascend's accounting MIB. Once sent, new overwrites will not cause another trap to be sent until at least one table's worth of new events has occurred.

Port state change events

Port state change event traps are effective on a port-by-port basis for each port pointed to by `ifIndex`. The `hostPort` objects are used to associate a change with `ifIndex` objects.

The following trap types signify a change in the state of the Ascend Inverse Multiplexer (AIM) port associated with the passed index.

Trap type	Indicates that the indexed AIM port
portInactive (ascend trap-type 0)	Has become inactive.
portDualDelay (ascend trap-type 1)	Is delaying the dialing of a second to avoid overloading devices that cannot handle two calls in close succession.
portWaitSerial (ascend trap-type 2)	Detects DTR and is waiting for an HDLC controller to come online. CTS is off (V.25 bis dialing only).
portHaveSerial (ascend trap-type 3)	Is waiting for V.25 bis commands. CTS is on.

Trap type	Indicates that the indexed AIM port
portRinging (ascend trap-type 4)	Has been notified of an incoming call.
portCollectDigits (ascend trap-type 5)	Is receiving digits from an RS366 interface (RS-366 dialing only).
portWaiting (ascend trap-type 6)	Is waiting for connect notification from the WAN after dialing or answer notification has been issued.
portConnected (ascend trap-type 7)	Has changed state. This change of state can be from connected to unconnected or vice versa. If connected to the far end, end-to-end data can flow but has not yet been enabled. The following trap report sequence shows that a link is up: portWaiting (6) portConnected (7) portCarrier (8) The following trap report sequence shows that a link is down: portConnected (7) portInactive (0)
portCarrier (ascend trap-type 8)	Has end-to-end data flow enabled.
portLoopback (ascend trap-type 9)	Has been placed in local loopback mode.
portAcrPending (ascend trap-type 10)	Has set ACR on the RS366 interface, and is waiting for the host device (RS-366 dialing only).
portDTENotReady (ascend trap-type 11)	Is waiting for DTE to signal a ready condition when performing X.21 dialing.

Security events

Security events are used to notify users of security problems and track access to the unit from the console. The MIB-II event *authenticationError* is a security event. The other security events are Ascend-specific. The include:

Security event	Signifies
authenticationFailure (RFC-1215 trap-type 4)	The DSL Terminator sending the trap is the addressee of a protocol message that is not properly authenticated.
consoleStateChange (ascend trap-type 12)	The console associated with the passed console index has changed state. To read the console's state, get `ConsoleEntry` from the Ascend enterprise MIB.
portUseExceeded (ascend trap-type 13)	The serial host port's use exceeds the maximum set by the Max DS0 Mins Port parameter associated with the passed index (namely, the interface number).
systemUseExceeded (ascend trap-type 14)	The serial host port's use exceeds the maximum set by the Max DS0 Mins System parameter associated with the passed index (namely, the interface number).

Security event	Signifies
maxTelnetAttempts (ascend trap-type 15)	A user has failed in three consecutive attempts to log into this DSL Terminator via Telnet.

Supported MIBs

You can download the most up-to-date version of the Ascend Enterprise MIB by logging in as `anonymous` to `ftp.ascend.com`. (No password is required.) In addition to the Ascend MIB, the DSL Terminator also supports objects related to Ascend functionality in the following Internet standard MIBs:

- MIB-II implementation (RFC 1213)
- DS1 MIB implementation (RFC 1406)
- RS232 MIB implementation (RFC-1317)
- Frame Relay MIB implementation (RFC-1315)
- DS3 and E3 management MIB implementation (RFC 1407)
- Bridge MIB implementation (RFC1493)
- Modem MIB implementation (RFC 1696)

You can download the most recent version of these RFCs by logging in as `anonymous` to `ftp.ds.internic.net`. (No password is required.)

Configuring Syslog

You can configure the DSL Terminator to send messages containing call and system events to an IP host running a syslog daemon.

To configure Syslog support, you must set parameters specifying the IP address of the host running the Syslog daemon. In addition, there are optional parameters you can set to customize the way the DSL Terminator sends its Syslog messages.

The IP host running the Syslog daemon is typically a UNIX host, but can be a Microsoft Windows workstation or server. If the DSL Terminator is on a different network than the IP host, you must configure the routers so that the DSL Terminator can successfully communicate with the IP host.

Note: Do not configure the DSL Terminator to send reports to a IP host that can be reached only by means of a dial-up connection.

Configuring to send Syslog messages

To configure the DSL Terminator to send messages to a Syslog daemon:

1. Open the Ethernet > Mod Config > Log menu.
2. Set the Syslog parameter to `Yes`.
3. Set Log Host to the IP address of the host running the syslog daemon.
4. Set Log Port to the port at which the syslog daemon listens for Syslog messages from the DSL Terminator. The default is 514.

5 Set the Log Facility value to be attached to each Syslog message.

The syslog daemon can receive messages from several devices, and it groups the messages. If the daemon receives messages from devices that specify the same log facility, it stores them in the same file.

6 Exit and save the changes.

To configure the syslog daemon on a UNIX host, you need to modify the host's `/etc/syslog.conf` file. This file specifies a specific action the daemon performs when it receives messages with a particular Log Facility number. For example, if you set Log Facility to Local5 in the DSL Terminator, and the `syslog` daemon should store messages from the DSL Terminator in the file `/var/log/`DSL Terminator, add the following line to the `/etc/syslog.conf` file:

`local5.info` *`tab`* `/var/log/DSL Terminator`

Note: After making changes to the /etc/syslog.conf file, you must direct the UNIX host to reread the file.

Syslog message format

DSL Terminator units generate Syslog messages in the following format:

`date time router_name` `ASCEND:` *`message`*

where:

Field	Description
`date`	The date the message was logged by the syslog daemon. The DSL Terminator does not datestamp the Syslog messages.
`time`	The time the message was logged by the syslog daemon. The DSL Terminator does not timestamp the syslog messages.
`router_name`	The name of the DSL Terminator sending the message.
`message`	The specific activity that caused the DSL Terminator to send the Syslog packet.

Syslog messages and their meanings

Syslog messages are recorded during establishment of a connection, during graceful or unexpected disconnection and during various other events.

In a Syslog message, `slot` *`x`* `port` *`y`* indicates that action occurred in a session with the module (slot card) located in slot `x`. Because slot cards support multiple simultaneous sessions, the DSL Terminator assigns the session to a specific port. For digital connections, port typically indicates an HDLC channel on an Ethernet card or Ether-Data card, although port can indicate a port on a slot card supporting inverse multiplexing.

LAN security error, Modem *x*:*y*—The DSL Terminator received a call on modem *y* in the module in slot *x*. The call has failed either because authentication failed, or because the IP address of the user did not match the IP address configured in the user's profile.

No connection—There was no response from the far end unit when the DSL Terminator attempted to connect.

No Channel Avail—*All* channels on the DSL Terminator are either supporting active connections or are disabled.

No Chan Other End—The unit that DSL Terminator is attempting to connect with did not have an available channel on which to answer the call.

Network Problem—The network has reported a protocol error.

Far End Hung Up—The network notified the DSL Terminator that the calling unit has disconnected the call.

Remote Mgmt Denied—A user attempted to initiate a remote management session, which was denied by the far end unit.

Incoming Net-2-Net—The DSL Terminator received an incoming Net-2-Net call.

Sys user exceeded—The DSL Terminator dropped the call because the call had exceeded the configured maximum system DS0 minutes.

Port use exceeded—The DSL Terminator dropped the call because the call had exceeded the maximum port DS0 minutes specified in the Port profile.

High Bit Errors—During a Bit Error Rate Test (BERT), the DSL Terminator detected a high number of bit errors.

Normal Bit Errors—During a Bit Error Rate Test (BERT), the DSL Terminator detected a normal number of bit errors.

No Trunk Available—The DSL Terminator has no active WAN links.

Trunk Down—A WAN link has gone down.

Trunk Up—A WAN link has become active.

Ethernet Up—The Ethernet interface of the DSL Terminator has become active or been re initialized. This message is logged when the Ethernet interface first comes up, or on the basis of a change to the Ethernet interface.

IP address 0.0.0.0 not valid for login service—A user attempted to initiate a login service with an invalid IP address.

TACACS+:No more TCP sockets—The DSL Terminator could not initiate a TACACS+ session.

TACACS+:Unexpected TCP close event. Server down?—The DSL Terminator received a TCP Close packet before the TACACS+ TCP session was established.

TACACS+:Resource shortage—The DSL Terminator experienced a low memory condition while processing TACACS+ session.

TACACS+:Shutdown in read—The DSL Terminator experienced an unexpected end to a TACACS+ session.

TACACS+:Server timeout—The DSL Terminator timed out while waiting to connect to the TACACS+ server.

TACACS+:Table exhausted—The DSL Terminator has no available entries in its TACACS+ entry table.

TACACS+:Illegal server response—The DSL Terminator received an illegal response from the TACACS+ server.

Backoff Q full, discarding user 10.10.10.1[250725066]—Backoff-queue overflow has resulted in silent discarding of the oldest entry. When a RADIUS accounting event occurs, the DSL Terminator (the NAS) sends an Accounting-Request message to the RADIUS Accounting server, which sends back an Accounting-Response message to acknowledge receipt. The NAS is required to buffer the event until it receives an acknowledgment. The NAS employs a simple exponential backoff algorithm between reattempts. The backoff algorithm is:

```
backoff_time = 3 * backoff_time
```

where `backoff_time = [1..N]`

Once the NAS sends an accounting request, if no response is received from the Accounting server, the NAS enters backoff mode.

If the backoff queue is not empty when an accounting event occurs (a new user logs in or an existing user logs out), the event goes directly onto the backoff queue.

A maximum of 100 entries is allowed on the backoff queue. If the queue overflows. the oldest entry is silently discarded, and the DSL Terminator sends the Syslog message.

The backoff queue can be cleared by setting Acct = None on the DSL Terminator or by resetting the DSL Terminator.

When you see this Syslog message, your Accounting Server is not functioning properly. If `Acct = RADIUS` on the DSL Terminator, verify that you are using the correct Port number (e.g. 1646) and that the Acct Key matches the password in the clients file on the RADIUS server. Also, be aware that the default location for your accounting records is `/usr/adm/radacct`. You have to create the `radacct` directory. RADIUS will automatically create a subdirectory with the name or IP address of the DSL Terminator (depending on your entry in the clients file) and will then write to the `detail` file. You can redirect your accounting output by starting RADIUS with the `-a` option (for example, `radiusd -a /usr/adm/ascendlog`).

Disconnect codes and progress codes

When a call disconnects, the DSL Terminator typically sends the following message:

`call` *`n`* `CL OK u=` *`username`* `c=`*`n`* `p=`*`m`*

where:

- *n* specifies a disconnect code indicating why the call disconnected.
- *m* specifies a progress code indicating how far the call had progressed when it disconnected.

Disconnect codes and their meanings

Following is a list of disconnect codes and their meanings:

Disconnect code	Description
1	Not applied to any call.
2	Unknown disconnect.
3	Call disconnected.
4	CLID authentication failed.
5	RADIUS timeout during authentication.
6	Successful authentication. DSL Terminator is configured to call the user back.
7	Pre-T310 Send Disc timer triggered.
9	No modem is available to accept call.
10	Modem never detected Data Carrier Detect (DCD).
11	Modem detected DCD, but modem carrier was lost.
12	DSL Terminator failed to successfully detect modem result codes.
13	DSL Terminator failed to open a modem for outgoing call.
14	DSL Terminator failed to open a modem for outgoing call while `ModemDiag` diagnostic command is enabled.
20	User exited normally from the terminal server.
21	Terminal server timed out waiting for user input.
22	Forced disconnect when exiting Telnet session.
23	No IP address available when invoking PPP command.
24	Forced disconnect when exiting raw TCP session.
25	Exceeded maximum login attempts.
26	Attempted to start a raw TCP session, but raw TCP is disabled on DSL Terminator.
27	Control-C characters received during login.
28	Terminal-server session cleared ungracefully.
29	User closed a terminal-server virtual connection normally.
30	Terminal-server virtual connect cleared ungracefully.
31	Exit from Rlogin session.
32	Establishment of rlogin session failed because of bad options.
33	DSL Terminator lacks resources to process terminal-server request.

Disconnect code	Description
35	MP+ session cleared because no null MP packets received. A DSL Terminator sends (and should receive) null MP packets throughout an MP+ session.
40	LCP timed out waiting for a response.
41	LCP negotiations failed, usually because user is configured to send passwords via PAP, and DSL Terminator is configured to only accept passwords via CHAP (or vice versa).
42	PAP authentication failed.
43	CHAP authentication failed.
44	Authentication failed from remote server.
45	DSL Terminator received Terminate Request packet while LCP was in open state.
46	DSL Terminator received Close Request from upper layer, indicating graceful LCP closure.
47	DSL Terminator cleared call because no PPP Network Core Protocols (NCPs) were successfully negotiated. Typically, there is no agreement on the type of routing or bridging that is supported for the session.
48	Disconnected MP session. The DSL Terminator accepted an added channel, but cannot determine the call to which to add the new channel.
49	Disconnected MP call because no more channels can be added.
50	Telnet or raw TCP session tables full.
51	DSL Terminator has exhausted Telnet or raw TCP resources.
52	For Telnet or raw TCP session, IP address is invalid.
53	For Telnet or raw TCP session, DSL Terminator cannot resolve hostname.
54	For Telnet or raw TCP session, DSL Terminator received bad or missing port number.
60	For Telnet or raw TCP session, host reset.
61	For Telnet or raw TCP session, connection was refused.
62	For Telnet or raw TCP session, connection timed out.
63	For Telnet or raw TCP session, connection closed by foreign host.
64	For Telnet or raw TCP session, network unreachable.
65	For Telnet or raw TCP session, host unreachable.
66	For Telnet or raw TCP session, network admin unreachable.
67	For Telnet or raw TCP session, host admin unreachable.
68	For Telnet or raw TCP session, port unreachable.
100	Session timed out.
101	Invalid user.
102	Callback enabled.
105	Session timeout on the basis of encapsulation negotiations.
106	MP session timeout.

Disconnect code	Description
115	Instigating call no longer active.
120	Requested protocol is disabled or unsupported.
150	Disconnect requested by RADIUS server.
151	Call disconnected by local administrator.
152	Call disconnected via SNMP.
160	Exceeded maximum number of V.110 retries.
170	Timeout waiting to authenticate far end.
180	User disconnected by executing Do Hangup from VT100 interface.
181	Call cleared by DSL Terminator.
185	Signal lost from far end, typically because the far end modem was turned off.
190	Resource has been quiesced.
195	Maximum duration time reached for call.
201	DSL Terminator has low memory.
210	DSL Terminator modem card stops working while it has calls outstanding.
220	DSL Terminator requires CBCP, but client does not support it.
230	DSL Terminator deleted Vrouter.
240	DSL Terminator disconnected call on the basis of LQM measurements.
241	DSL Terminator cleared backup call.
250	IP FAX call cleared normally.
251	IP FAX call cleared because of low available memory.
252	DSL Terminator detected an error for an incoming IP FAX call.
253	DSL Terminator detected an error for an outgoing IP FAX call.
254	DSL Terminator detected no available modem to support an IP FAX call.
255	DSL Terminator detected problem opening IP FAX session.
256	DSL Terminator detected a problem when performing a TCP function during an IP FAX call.
257	IP FAX session cleared abnormally.
258	DSL Terminator detected problem when parsing telephone number for IP FAX call.
260	DSL Terminator detected problem when decoding IP FAX variables.
261	DSL Terminator detected problem when decoding IP FAX variables.
262	DSL Terminator has no configured IP FAX server.
300	DSL Terminator detects X.25 error.

Progress codes and their meanings

Following are the progress codes and their meanings:

Progress code	Description
1	Not applied to any call.
2	Unknown progress.
10	DSL Terminator has detected and accepted call.
30	DSL Terminator has assigned modem to call.
31	Modem is awaiting DCD from far-end modem.
32	Modem is awaiting result codes from far-end modem.
40	Terminal-server session started.
41	Raw TCP session started.
42	Immediate Telnet session started.
43	Connection made to raw TCP host.
44	Connection made to Telnet host.
45	Rlogin session started.
46	Connection made with Rlogin session.
47	Terminal-server authentication started.
50	Modem outdial session started.
60	LAN session is up.
61	Opening LCP.
62	Opening CCP.
63	Opening IPNCP.
64	Opening BNCP.
65	LCP opened.
66	CCP opened.
67	IPNCP opened.
68	BNCP opened.
69	LCP in Initial state.
70	LCP in Starting state.
71	LCP in Closed state.
72	LCP in Stopped state.
73	LCP in Closing state.
74	LCP in Stopping state.
75	LCP in Req-Sent state.
76	LCP in Ack-Rcvd state.
77	LCP in Ack-Sent state.
80	IPX NCP in Open state. (IPX does not apply to DSL Terminator.)
81	AT NCP in Open state.

Progress code	Description
82	BACP being opened.
83	BACP is now open.
84	CBCP being opened.
85	CBCP is now open.
90	DSL Terminator has accepted V.110 call.
91	V.110 call in Open state.
92	V.110 call in Carrier state.
93	V.110 call in Reset state.
94	V.110 call in Closed state.
100	DSL Terminator determines that call requires callback.
101	Authentication failed.
102	Remote authentication server timed out.
120	Frame Relay link is inactive. Negotiations are in progress.
121	Frame Relay link is active and has end-to-end connectivity.
200	Starting Authentication layer.
201	Authentication layer moving to opening state.
202	Skipping Authentication layer.
203	Authentication layer in opened state.

Troubleshooting

A

Indicator Lights

Lights (LEDs) on the DSL Terminator front and back panel indicate the status of the unit.

Front panel

The front-panel LEDs indicate the status of the system, the PRI interface, and the data transfer in active sessions.

Table A-1 lists and describes each LED.

Table A-1. DSL Terminator front-panel status lights

Status light	Description
Power	On when the DSL Terminator power is on.
Fault	On in one of two cases: A hardware self-test in progress or a hardware failure. At system start-up, when the DSL Terminator performs its Power On Self Test (POST), the status light is on. If any type of hardware failure occurs, the status light flashes. If the failure is isolated to a slot card, the DSL Terminator might continue to function without the card.
Alarm	On when the ambient temperature inside the unit exceeds 65 C.
Eth-Link1	On when the DSL Terminator detects activity (network traffic) on its first Ethernet interface.
Eth-Link2	On when the DSL Terminator detects activity (network traffic) on its second Ethernet interface.
Eth-Act1	On when there is activity on the first Ethernet link.

Table A-1. DSL Terminator front-panel status lights (continued)

Status light	Description
Eth-Act2	On when there is activity on the first Ethernet link.
Coll 1	On if there are collisions on the first Ethernet link.
Coll 2	On if there are collisions on the second Ethernet link.

DSL Terminator back-panel

Table A-2 describes the DSL Terminator backpanel status lights, which display the status of the Ethernet– interface.

Table A-2. DSL Terminator backpanel status lights

Status light	Description
Eth-Link1	On when the DSL Terminator detects activity (network traffic) on its first Ethernet interface.
Eth-Link2	On when the DSL Terminator detects activity (network traffic) on its second Ethernet interface.
Wan *n*	
Eth-Act1	On when there is activity on the first Ethernet link.
Eth-Act2	On when there is activity on the first Ethernet link.

Interpreting the DS3-ATM card's status lights

All status lights except LA, are lit when power is turned on or card is reset and remain so until the card passes POST. If no status lights are lit, the DS3 interface is either disabled or is receiving an Alarm Indication Signal (AIS) or Idle Signal.

Table A-3 explains the DS3-ATM card status lights.

Table A-3. ATM-DS3 card status lights

Lights	Description
LA	Green. Indicates the DS3 interface is enabled and has not detected any error conditions.
RA	Red. Indicates the DS3 interface is experiencing loss of receive signal.
LO	Red. Indicates the DS3 interface is out of frame alignment.
YA	Yellow. Indicates the DS3 interface has detected Far End Receive Failure indication transmitted from the other side.

Interpreting the UDS3 card's status lights

All status lights, except LA are lit when power is turned on or card is reset and remain so until the card passes POST. If no status lights are lit, the DS3 interface is either disabled or is receiving an Alarm Indication Signal (AIS) or Idle Signal.

Table A-4 explains the UDS3 card status lights.

Table A-4. UDS3-card status lights

Lights	Description
LA	Green. Indicates the DS3 interface is enabled and has not detected any error conditions.
RA	Red. Indicates the DS3 interface is experiencing loss of receive signal.
LO	Red. Indicates the DS3 interface is out of frame alignment.
YA	Yellow. Indicates the DS3 interface has detected Far End Receive Failure indication transmitted from the other side.

Interpreting the OC3-ATM card's status lights

All status lights, except LA, are lit when power is turned on or card is reset and remain so until the card passes POST. If no LEDs are lit, the OC3 interface is disabled.

Table A-5 explains the OC3-ATM card status lights.

Table A-5. OC3-ATM card status lights

Lights	Description
LA	Green. Indicates the OC3 interface is enabled and has not detected any error conditions.
LO	Red. Indicates the OC3 interface is out of frame alignment.
RA	Red. Indicates the OC3 interface is experiencing loss of receive signal.
YA	Yellow. Indicates the OC3 interface has detected Far End Receive Failure indication transmitted from the other side.
AD	Alarm Indication Signal. Indicates the local device has received an alarm indication signal. Also known as a blue alarm.

Common problems and their solutions

This section lists problems you might encounter and describes ways to resolve them. It categorizes common problems as general problems, configuration problems, hardware configuration problems, and problems indicated by the LEDs.

General problems

When the list of DO commands appears, many operations might not be not available if the right profile has not been selected. Because the DSL Terminator can manage a number of calls simultaneously, you might need to select a specific Connection profile, Port profile, or Call profile in order to see certain DO commands. For example, to dial from a Call profile or a Connection profile, you must move to the Call profile (Host/6 > Port *N* Menu > Directory) or the Connection profile and press Ctrl-D 1.

Note that you cannot dial if `Operations=No` for the control port. If a call is already active, DO 2 (Hang Up) appears instead of DO 1 (Dial). If the T1 or E1 line is not available, Trunk Down appears in the message log and you cannot dial.

Configuration problems

The most common problems result from improperly configured profiles.

The DSL Terminator cannot dial out on a T1 or E1 line

To verify that the configured profile is correctly configured:

1. Make certain that you have entered the correct phone number to dial.
2. Verify that the Data Svc parameter specifies a WAN service available on your line.
   If you request a WAN service that is not available on your line, the WAN rejects your request to place a call.
3. Check whether the channels using the requested WAN service are busy.
   If these channels are busy, an outgoing call might be routed to channels for which you did not request the specified WAN service. Check the Data Svc, Call-by-Call, and PRI # Type parameter values in the profile.
4. Determine whether you have correctly set the parameters controlling Dynamic Bandwidth Allocation.
   For detailed information, see the *Network Configuration Guide* for your DSL Terminator.

Restored configuration has incorrect RADIUS parameters

On earlier RADIUS Servers, the submenu consisted of three clients (specific host addresses) and one Server Key for all three clients. If the DSL Terminator supports the new RADIUS Server, the restoration of the DSL Terminator configuration will cause a problem, because the new RADIUS Server allows up to nine addresses (host or net) and a Server Key for each address. When you restore configurations with the old Client Address list, the subnet mask assigned to the clients will be the default subnet mask of the address type given (for example, 128.50.1.1 will get a subnet mask of 16) and not the previous 32-bit (single host) address. In addition, the Server Key will not automatically be set. You must set the Server Key manually for each client in the RADIUS Server submenu.

Hardware configuration problems

If you cannot communicate with the DSL Terminator through the VT100 control terminal, you might have a problem with terminal configuration, the control port cable, or the DSL Terminator hardware.

Cannot access the VT100 interface

If no data is displayed on the VT100 interface, verify that the unit completes all of the Power-On Self Tests (POST).

For information, see the *Hardware Installation Guide* for your DSL Terminator.

Random characters appear in the VT100 interface

If random or illegible characters appear on your display, you probably have a communications settings problem. Specify the following settings:

- 9600 bps data rate
- 8 data bits
- 1 stop bit
- No flow control
- No parity

If you have changed the data rate through the Port profile, make certain that your VT100 terminal matches that rate.

A Power-On Self Test fails

If the start-up display indicates a failure in any part of the POST, an internal hardware failure has occurred with the unit. In this case, contact Lucent Customer Service.

Bridge/router problems

Problems with a bridge or router can include the uncertainty of link quality and the DSL Terminator hanging up after answering an IP call.

The link is of uncertain quality

When running File Transfer Protocol (FTP), the data transfer rate appears in bytes per second. Multiply this rate times 8 to get the bits per second. For example, suppose that you are connected to Detroit on a 56-Kbps B channel and that FTP indicates a 5.8 Kbyte/s data rate. In this case, the link is running at 5.8x8=46.8 Kbps, or approximately 83% efficiency. Many factors can affect efficiency, including the load on the FTP server, the round-trip delay, the overall traffic between endpoints, and the link quality.

You can check link quality in the WAN Stat status window, or by running a Ping between the same endpoints. Dropped packets hurt the link's efficiency, as does round-trip delay. Random round-trip delay indicates heavy traffic, a condition that also drops the efficiency of the link.

The DSL Terminator hangs up after answering an IP call

If the DSL Terminator hangs up after answering an IP call, proceed as follows:

1 If you are running PPP, verify that you have entered the proper passwords.

2 Verify that Auth is set to PAP or CHAP.

3 If you are routing IP over PPP, verify that the calling device gives its IP address

Some calling devices supply their names, but not their IP addresses. However, you can derive an IP address if the calling device is listed in a local Connection profile or on a RADIUS authentication server. Try enabling PAP or CHAP for the Recv Auth parameter so that the DSL Terminator matches the caller's name to the Station parameter in a Connection profile and gets the corresponding LAN Adrs.

Diagnostic Command Reference

B

The diagnostic commands usually provide information about the unit, the interface or its connections. This information can help you determine where the problems are. Under most circumstances, diagnostic commands are not required for correct operation of the DSL Terminator. In some circumstances, using these commands might produce undesirable results.

All available information about the DSL Terminator diagnostic commands is listed here. It is organized alphabetically for quick reference, and does not include tutorials. Use the following information with caution. Contact Lucent Technical Support with any questions or concerns. This guide provides

Note: Every attempt has been made to confirm that this chapter correctly describes the functionality and output of the DSL Terminator diagnostic commands. But while diagnostic mode can be a very valuable troubleshooting tool for anyone, its primary focus is on the requirements of Lucent's development engineers. For this reason, Lucent does not guarantee the completeness of the list of commands or of the cataloging of functionality from release to release.

Using diagnostic commands

To be allowed access to diagnostic mode, you must set the Field Service privilege to `Yes` in the active Security profile.

Use one of the following two methods to access diagnostic mode:

- From the DSL Terminator VT100 interface, display the DO menu by pressing Ctrl-D. Then press D or select D=Diagnostics.
- From the DSL Terminator VT100 interface, type the following key sequence in rapid succession:

  `Esc [ Esc =`

  (Press the Escape key, followed by the Left Bracket key, then the Escape key again, followed by the = key.)

  You must press all four keys within one second for the DSL Terminator to recognize the escape sequence.

To display an abbreviated list of the most commonly used commands in diagnostic mode, enter a question mark:

```
>?
```

To display a complete listing, append **ascend** to the question mark:

```
>? ascend
```

To exit diagnostic mode, enter **quit**.

Because most diagnostic commands are designed to give a developer information about specific aspects of DSL Terminator functionality, you might find it helpful to use commands in combination to troubleshoot different problems.

For example, when troubleshooting modem-related issues, you might want to use ModemDrvState, ModemDiag, and MDialout (if modem dial-out is supported on your DSL Terminator) to get all modem-related information for your calls.

Using several commands simultaneously not only gives you a clearer picture of what is happening, but also shows you a chronological timeline of the events.

Command reference

Every attempt has been made to describe the output and functionality of the diagnostic commnds correctly, However, Lucent does not guarantee the completeness of the command list of description of the functionality because they can vary from release to release

Following are the DSL Terminator diagnostic commands in alphabetic order:

?

Description: Displays an abbreviated list of the most commonly used diagnostic commands and a brief description of each command.

Example:

```
> ?
? -> List all monitor commands
clr-history -> Clear history log
dnldCode -> download code from serial port
ether-display -> ether-display <port #> <n>
fatal-history -> List history log
fclear -> clear configuration from flash
frestore -> restore configuration from flash
fsave -> save configuration to flash
FWALLdblog -> Inquire/change firewall debug logging
FWALLversion -> Display firewall software version number
help -> List all monitor commands
nslookup -> Perform DNS Lookup
```

```
quit -> Exit from monitor to menus
reset -> Reset unit
tloadcode -> load code from tftp host
trestore -> restore configuration from tftp host
tsave -> save configuration to tftp host
wanDisplay -> wanDisplay <n>
wanDSess -> wandsess <sess <n>> (display per session)
wanNext -> wanNext <n>
< -- Hit [return] for next page, q [return] to end list  -- >
wanOpening -> wanOpening <n> (displays packets during opening/nego-
tiation)
```

Usage: Append certain commands with the ? character to display help for that command.

Syntax element	Description
`tshow ?`	`tsShow -> Show various tables. Type 'tsshow ?' for help.`

Example:

```
> tsShow ?
tsshow ?            Display help information
tsshow uptime       Display system uptime.
tsshow revision     Display system revision.
```

See Also: Help

ARPTable

Description: Displays the DSL Terminator's Address Resolution Protocol (ARP) table. The DSL Terminator uses the ARP table to associate known IP addresses with physical hardware addresses.

Usage: **`arptable`**

Example:

```
DSL Terminator> arptable
         ip address   ether addr  if rts pkt   ref  insert
DYN    206.30.33.11 00A0244CCE04   0   0   0     1   281379
DYN   206.30.33.254 00605C4CA220   0   0   0     1   281303
DYN    206.30.33.21 00059A403B47   0   0   0     1   281179
DYN    206.30.33.15 00A0247C2A72   0   0   0     1   281178
```

The ARP table displays the following information:

Column	Description
	Unnamed first column indicates how the address was learned, dynamically (DYN) or by specification of a Bridge Address (STA).
`ip address`	Network address contained in ARP requests.
`ether addr`	Media Access Control (MAC) address of the host identified by `ip address`. Also referred to as the hardware address.
`if`	Interface on which the DSL Terminator received the ARP request.
`rts`	Routes pointing to the address.
`pkt`	Number of packets queued.
`ref`	Number of times that the address was used.
`insert`	Time at which this entry was inserted into the ARP table.

Callback

Description: Displays messages related to the callback functionality of the DSL Terminator. You can use the command to display, for example, sessions queued for callback. The command is a toggle that alternately enables and disables the debug display.

With the callback feature enabled, the DSL Terminator hangs up after receiving an incoming call that matches the specifications in the Connection profile. The DSL Terminator then uses the Dial # parameter specified in the Connection profile to call back the device at the remote end of the link.

You can use the callback command to tighten security by ensuring that the DSL Terminator connects to known destinations only. The command can also help you troubleshoot detailed areas of the callback process.

Usage: `callback`

Example: Following are several examples of output displayed by the Callback command.

```
> callback
CALLBACK debug is now ON
```

The following message appears as the DSL Terminator prepares to call back the remote end:

```
CALLBACK: processing entry topeka
```

The DSL Terminator then dials the remote end:

```
CALLBACK: initiate call to topeka
```

When the call has been made and is being negotiated:

```
CALLBACK: new state WAITING
```

If callback failed and will be retried:

```
CALLBACK: new state FAILED
```

If callback is never successful, the call is marked for removal from the callback list and the following message appears:

```
CALLBACK-FAILED: topeka marked as failed
```

After the remote end is called back, its entry is removed from the Callback list so that the DSL Terminator can reallocate and use the resources. The following message appears:

```
CALLBACK: deleting entry topeka
```

To terminate the display:

```
> callback
CALLBACK debug is now OFF
```

Clr-History

Description: Clears the fatal-error history log.

Usage: **`clr-history`**

To display the log before clearing it, enter the Fatal-History command.

Example:

```
> fatal-history
OPERATOR RESET:  Index: 99  Load: ti.m40 Revision: 5.0A
Date: 02/13/1997.       Time: 04:22:47
DEBUG Reset from unknown in security profile 1.
SYSTEM IS UP:  Index: 100  Load: ti.m40 Revision: 5.0A
Date: 02/13/1997.       Time: 04:23:50
> clr-history
```

The log is now empty:

```
> fatal-history
>
```

See Also: Fatal-History

Ether-Display

Description: Displays the contents of Ethernet packets.

If you enter the command while traffic through your DSL Terminator is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message **`----- data lost -----`**, which just means that not all the output can be displayed on the screen. You might prefer to use the Ether-Display command during a period of low activity.

Usage: ether-display *port 0-#* *n*

Syntax element	Description
port 0-#	The range of Ethernet ports on which received or transmitted packets should be displayed. Use zero only to indicate that Ethernet packets for all ports should be displayed.
n	The number of octets to display from each Ethernet packet.

Example: To display the first 12 octets of each Ethernet packet for all ports:

```
> ether-display 0 12
Display the first 12 bytes of ETHER messages
ETHER XMIT: 105 octets @ B07BE920
[0000]: 00 40 C7 5A 64 6C 00 C0 7B 0C 01 59
ETHER RECV: 64 octets @ B077EE70
[0000]: 00 C0 7B 0C 01 59 00 40 C7 5A 64 6C
ETHER XMIT: 219 octets @ B07BE920
[0000]: 00 40 C7 5A 64 6C 00 C0 7B 0C 01 59
ETHER RECV: 64 octets @ B077F4C0
[0000]: 00 C0 7B 0C 01 59 00 40 C7 5A 64 6C
> ether-display 0 0
ETHER message display terminated
```

Fatal-History

Description: Displays the fatal-error log. Each time the DSL Terminator reboots, it logs a fatal-error message to the fatal-error history log. The fatal-error log also includes Warnings, for which the DSL Terminator did not reset. Development engineers use Warnings for troubleshooting purposes. A Warning indicates that the DSL Terminator detected an error condition but recovered from it. The number of entries in this log is limited by available flash space, and the errors rotate on a First-In, First-Out (FIFO) basis. You can use the Clr-History command to clear the log.

Note: If your DSL Terminator experiences a fatal-error reset or Warning, contact Lucent Technical Support immediately.

Usage: fatal-history

Example:

```
> fatal-history
OPERATOR RESET:  Index: 99  Load: ti.m40 Revision: 5.0A
Date: 02/13/1997.       Time: 04:22:47
DEBUG Reset from unknown in security profile 1.
SYSTEM IS UP:  Index: 100  Load: ti.m40 Revision: 5.0A
Date: 02/13/1997.       Time: 04:23:50
```

Definitions of fatal errors:

The following reset is the result of an Assert. This problem can be either hardware or software related. Contact Lucent Technical Support if you experience an FE1 reset.

```
FATAL_ASSERT =              1
```

The following reset results from an out-of-memory condition, sometimes termed a memory leak:

```
FATAL_POOLS_NO_BUFFER =     2
```

Other resets include:

```
FATAL_PROFILE_BAD =         3
FATAL_SWITCH_TYPE_BAD =     4
FATAL_LIF_FATAL =           5
FATAL_LCD_ERROR =           6
FATAL_ISAC_TIMEOUT =        7
FATAL_SCC_SPURIOUS_INT =    8
```

The preceding reset is caused by a processor exception error.

```
FATAL_EXEC_INVALID_SWITCH = 9
FATAL_EXEC_NO_MAIL_DESC =   10
```

The preceding reset occurs if the DSL Terminator tries to allocate a mail message and there are none left. A reset of this type is usually due to a memory leak.

```
FATAL_EXEC_NO_MAIL_POOL =   11
FATAL_EXEC_NO_TASK =        12
FATAL_EXEC_NO_TIMER =       13
FATAL_EXEC_NO_TIMER_POOL =  14
FATAL_EXEC_WAIT_IN_CS =     15
FATAL_DSP_DEAD =            16
FATAL_DSP_PROTOCOL_ERROR =  17
FATAL_DSP_INTERNAL_ERROR =  18
FATAL_DSP_LOSS_OF_SYNC =    19
FATAL_DSP_UNUSED =          20
FATAL_DDD_DEAD =            21
FATAL_DDD_PROTOCOL_ERROR =  22
FATAL_X25_BUFFERS =         23
FATAL_X25_INIT =            24
FATAL_X25_STACK =           25
FATAL_ZERO_MEMALLOC =       27
FATAL_NEG_MEMALLOC =        28
FATAL_TASK_LOOP =           29
```

The preceding reset is caused by a software loop.

```
FATAL_MEMCPY_TOO_LARGE =    30
FATAL_MEMCPY_NO_MAGIC =     31
FATAL_MEMCPY_WRONG_MAGIC =  32
FATAL_MEMCPY_BAD_START =    33
FATAL_IDEC_TIMEOUT =        34
FATAL_EXEC_RESTRICTED =     35
```

```
FATAL_STACK_OVERFLOW =      36
FATAL_OPERATOR_RESET =      99
```

The preceding entry is logged to the fatal-error table when the DSL Terminator has been manually reset, either in diagnostic mode (with the Reset or NVRAMclear commands), through the user interface, or through MIF.

Instead of a standard stack backtrace, the message includes the active Security profile index. On the DSL Terminator the Default profile is number 1, and the Full Access profile is number 9. 0 indicates an unknown security profile.

The reset is logged immediately before the DSL Terminator goes down.

```
FATAL_SYSTEM_UP =           100
```

As a complement to entry 99, the preceding entry is logged as the DSL Terminator is coming up. For a normal, manual reset, a fatal error 99 should appear, followed by a fatal error 100.

Warning messages

Warnings are not the result of reset conditions. The DSL Terminator logs Warnings when it detects a problem and recovers. Following are the Warnings, in numeric order:

```
ERROR_BUFFER_IN_USE             101
ERROR_BUFFER_WRONG_POOL         102
ERROR_BUFFER_WRONG_HEAP         103
ERROR_BUFFER_NOT_MEMALLOC       104
```

Warning 104 can be logged under different conditions (for example, double freeing memory or a low-memory condition).

```
ERROR_BUFFER_BAD_MEMALLOC       105
ERROR_BUFFER_BOGUS_POOL         106
ERROR_BUFFER_BOGUS_HEAP         107
```

Warning 107 indicates that memory management code (or other modules) detects that the buffer header of what should be a free buffer is corrupted by the previous overwrite.

```
ERROR_BUFFER_NEG_MEMALLOC       108
```

Warning 108 is logged when a negative length request is made to the memory allocation code.

```
ERROR_BUFFER_ZERO_MEMALLOC      109
```

Warning 109 is similar to Warning 108, except that the a zero length request is made to the memory allocation code.

```
ERROR_BUFFER_BOUNDARY           110
ERROR_BUFFER_TOO_BIG            111
```

Warning 111 occurs when a software routine has tried to allocate a block of memory greater than 64KB.

```
ERROR_BUFFER_NULL               112
ERROR_BUFFER_SEGCOUNT_ZERO      113
ERROR_BUFFER_TRAILER_MAGIC      114
ERROR_BUFFER_TRAILER_BUFFER     115
ERROR_BUFFER_TRAILER_LENGTH     116
```

```
ERROR_BUFFER_TRAILER_USER_MAGIC 117
ERROR_BUFFER_WRITE_AFTER_FREE   118
ERROR_BUFFER_NOT_IN_USE         119
ERROR_BUFFER_MEMCPY_MAGIC       120
ERROR_BUFFER_MEMCPY_MAGIC_NEXT  121
ERROR_BUFFER_MIN                101
ERROR_BUFFER_DSLMAX 121
ERROR_LCD_ALLOC_FAILURE         145
```

Warning 145 occurs when a memory-copy routine was called but the source buffer was much larger than expected.

```
ERROR_MEMCPY_TOO_LARGE          150
ERROR_MEMCPY_NO_MAGIC           151
ERROR_MEMCPY_WRONG_MAGIC        152
ERROR_MEMCPY_BAD_START          153
ERROR_WAN_BUFFER_LEAK           154
```

Warning 154 is caused by an error in the WAN driver.

```
ERROR_TERMSRV_STATE             160
ERROR_TERMSRV_SEMA4             161
ERROR_STAC_TIMEOUT              170
ERROR_EXEC_FAILURE              175
```

Warning 175 occurs because the kernel temporarily does not have available memory to spawn a task.

```
ERROR_EXEC_RESTRICTED           176
ERROR_EXEC_NO_MAILBOX           177
ERROR_EXEC_NO_RESOURCES         178
ERROR_CHAN_MAP_STUCK            180
```

Warning 180 is caused by a missing channel on a T1/PRI line.

```
ERROR_CHAN_DISPLAY_STUCK        181
ERROR_NEW_CALL_NO_DISC_REQ      182
```

Warning 182 indicates that a Disconnect message to the Central Office (CO) has not been sent. The problem can be caused by conditions on the DSL Terminator or at the CO. When the DSL Terminator encounters the condition, it assumes the CO is correct, and answers the call.

```
ERROR_NEW_CALL_NO_DISC_RESP     183
ERROR_DISC_REQ_DROPPED          184
ERROR_SPYDER_BUFFER             185
ERROR_SPYDER_DESC               186
ERROR_TCP_SBCONT_TOO_BIG        190
ERROR_TCP_SEQUENCE_GAP          191
ERROR_TCP_TOO_MUCH_DATA         192
ERROR_TCP_TOO_MUCH_WRITE        193
ERROR_TCP_BAD_OPTIONS           194
```

See Also: Clr-History

FClear

Description: Clears Flash memory on the DSL Terminator. When the DSL Terminator boots, it loads the code and configuration from Flash memory into Dynamic Random Access Memory (DRAM). If you want to return your DSL Terminator to its factory-set defaults, you need to perform an FClear.

Usage: **`fclear`**

Example:

```
> fclear
```

FRestore

Description: Restores a configuration from Flash memory and loads it into DRAM on the DSL Terminator.

Note: The DSL Terminator performs an FRestore when it boots. You need to execute the command if you have made changes to the current configuration and want to restore the configuration stored in Flash memory.

Usage: **`frestore`**

FSave

Description: Stores the current configuration into Flash memory.

Note: When you load code with the TloadCode command, an FSave is performed automatically before the code is uploaded. When the box boots after the upload, the DSL Terminator will load the configuration stored in Flash rather than be reset to factory default settings.

Usage: **`fsave`** .

Heartbeat

Description: Displays information related to multicast heartbeat functionality. The command is a toggle that alternately enables and disables the debug display.

Usage: **`heartbeat`** .

Example: Following are several examples of output displayed by the Heartbeat command.

```
HB: Sending SNMP Alarm count
HB: Checking Number of HeartBeats received
HB: HeartBeats received x
HB: Changing to Alarm Mode, HeartBeats Received x Expected y
HB: HeartBeat group address changed
HB: Heart beat received with invalid UDP port
HB: Heart beat received from invalid source
HB: Received HeartBeat packet
```

Help

Description: Displays a list of the most commonly used diagnostic commands and a brief description of each command. You can append the `ascend` modifier to display the complete list of commands.

Usage: `help` [`ascend`]

Syntax element	Description
`ascend`	List all commands.

Example:

```
> help
? -> List all monitor commands
clr-history -> Clear history log
dnldCode -> download code from serial port
ether-display -> ether-display <port #> <n>
fatal-history -> List history log
fclear -> clear configuration from flash
frestore -> restore configuration from flash
fsave -> save configuration to flash
FWALLdblog -> Inquire/change firewall debug logging
FWALLversion -> Display firewall software version number
help -> List all monitor commands
nslookup -> Perform DNS Lookup
quit -> Exit from monitor to menus
reset -> Reset unit
tloadcode -> load code from tftp host
trestore -> restore configuration from tftp host
tsave -> save configuration to tftp host
wanDisplay -> wanDisplay <n>
wanDSess -> wandsess <sess <n>> (display per session)
wanNext -> wanNext <n>
wanOpening -> wanOpening <n> (displays packets during
opening/negotiation)
```

See Also: ?

NSLookup

Description: Similar to the UNIX nslookup command. When you specify a host name, a DNS request is forwarded. If the host is found, the corresponding IP address is displayed.

Usage: `nslookup` *`host_name`*

Example:

```
> nslookup host1
Resolving host host1.
IP address for host drawbridge is 1.1.1.1.
> nslookup 198.4.92.1
Resolving host 198.4.92.1.
> nslookup
Missing host name.
> nslookup nohost
Resolving host nohost.
Unable to resolve nohost!
```

NVRAMClear

Description: Clears Nonvolatile Random Access Memory (NVRAM). The current system configuration is stored in NVRAM.

Note: A copy of the configuration may also be stored in Flash memory. If you clear NVRAM, the DSL Terminator resets and initializes itself with the configuration it detects in Flash memory. To return your DSL Terminator to its factory default settings, you must first use the FClear command to clear the configuration in Flash then use NVRAMClear.

Usage: `nvramclear` .

See Also: FClear

PPPDump

Description: Very similar to the WANDisplay diagnostic command. But PPPDump strips out escape characters that are present for asynchronous PPP users (who are dialing in with modems). The escape characters are necessary because of the asynchronous nature of the data stream. Stripping them out simply clarifies the presentation of the data.

If you enter the command while traffic through your DSL Terminator is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message `----- data lost -----`, which just means that not all the output can be displayed on the screen. You might prefer to use the PPPDump command during a period of low throughput.

`Usage: pppdump` *`n`*

where ***n*** is the number of octets to display per frame. Specifying a value of 0 (zero) disables the logging of data.

Example:

Consider the following frames, which were logged by the WANDisplay 64 command:

```
7E FF 7D 23 C0 21 7D 21 7D 21 7D 20 7D 37 7D 22 7D 26 7D 20 7D
2A 7D 20 7D 20 2D 7D 23 7D 26 3A AA 7E
7E FF 7D 23 C0 21 7D 21 7D 21 7D 20 23 7D 20 7D 24 7D 20 7D 20
7D 22 7D 7E
```

To get the data stream without escape characters, the 0x7D bytes need to be stripped, and the byte following each 0x7D byte needs to be decremented by 0x20.

With PPPDump, the DSL Terminator automatically convert and displays the data as follows:

```
7E FF 03 C0 21 01 01 00 17 02 06 00 0A 00 00 2D 03 06 3A AA 7E 7E
FF 03 C0 21 01 01 00 23 00 24 00 00 02 7E
```

See Also: WANDisplay, WANNext, WANOpen

PPPFSM

Displays changes to the PPP state machine as PPP users connect. The command is a toggle that alternately enables and disables the diagnostics display.

Usage: **`pppfsm`** .

Example: The following display shows the complete establishment of a PPP session.

```
> pppfsm
PPPFSM state display is ON
PPPFSM-97: Layer 0   State INITIAL     Event OPEN...
PPPFSM-97: ...New State STARTING
PPPFSM-97: Layer 0   State STARTING    Event UP...
PPPFSM-97: ...New State REQSENT
PPPFSM-97: Layer 1   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 2   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 3   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 4   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 5   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 6   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 7   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 8   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 9   State INITIAL     Event UP...
PPPFSM-97: ...New State CLOSED
PPPFSM-97: Layer 0   State REQSENT     Event RCONFREJ...
PPPFSM: irc_new scr 4
PPPFSM-97: ...New State REQSENT
PPPFSM-97: Layer 0   State REQSENT     Event RCONFACK...
PPPFSM-97: ...New State ACKRECD
PPPFSM-97: Layer 0   State ACKRECD     Event RCONFREQ...
PPPFSM-97: ...New State ACKRECD
PPPFSM-97: Layer 0   State ACKRECD     Event RCONFREQ...
PPPFSM-97: Layer 1   State CLOSED      Event OPEN...
PPPFSM-97: ...New State REQSENT
PPPFSM-97: ...New State OPENED
```

```
PPPFSM: PAP Packet
PPPFSM-97: Layer 6   State CLOSED      Event OPEN...
PPPFSM-97: ...New State REQSENT
PPPFSM-97: Layer 4   State CLOSED      Event OPEN...
PPPFSM-97: ...New State REQSENT
PPPFSM-97: Layer 4   State REQSENT     Event RCONFREQ...
PPPFSM-97: ...New State REQSENT
PPPFSM: ccp Packet code 1
PPPFSM-97: Layer 6   State REQSENT     Event RCONFREQ...
PPPFSM-97: ...New State REQSENT
PPPFSM: ccp Packet code 2
PPPFSM-97: Layer 6   State REQSENT     Event RCONFACK...
PPPFSM-97: ...New State ACKRECD
PPPFSM-97: Layer 4   State REQSENT     Event RCONFACK...
PPPFSM-97: ...New State ACKRECD
```

PPPIF

Description: Displays messages relating to each PPP connection. This command is particularly useful in troubleshooting negotiation failures. To help in troublshooting PPP issues, you might want to use PPPIF in conjunction with PPPDump.

Usage: **`pppif`** .

Example:

```
> pppif
PPPIF debug is ON
PPPIF: open: routeid 285, incoming YES
```

The following message indicates a modem call:

```
PPPIF-110: ASYNC mode
```

Link Compression Protocol (LCP) is negotiated:

```
VJ Header compression is enabled.
PPPIF-110: vj comp on
```

PAP authentication is configured on the DSL Terminator and required for access:

```
PPPIF-110: _initAuthentication
PPPIF-110: auth mode 1
PPPIF-110: PAP auth, incoming
PPPIF-110: bypassing async layer
```

LCP has been successfully negotiated and established. Authentication is next:

```
PPPIF-110: Link Is up.
PPPIF-110: pppMpNegUntimeout last 0 layer 0
PPPIF-110: pppMpNegUntimeout last 0 layer 0
PPPIF-110: LCP Opened, local 'Answer', remote ''
PPPIF-110: _openAuthentication
PPPIF-110: pppMpNegUntimeout last 0 layer 1
PPPIF-110: Auth Opened
PPPIF-110: Remote hostName is 'my_name'
```

PAP Authentication was successful. Compression Control Protocol (CCP) is negotiated next, along with IP Network Control Protocol (IPNCP):

```
PPPIF-110: opening CCP
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpNegTimeout layer 6
```

The user is given the address 1.1.1.1 from pool 0:

```
PPPIF-110: using address from pool 0
PPPIF-110: Allocated address [1.1.1.1]
PPPIF-110: opening IPNCP:
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpNegTimeout layer 4
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpNegUntimeout last 0 layer 6
PPPIF-110: pppMpNegUntimeout last 0 layer 4
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpNegUntimeout last 0 layer 4
PPPIF-110: IPNCP Opened to
PPPIF-110: pppMpSendNeg Pkt
PPPIF-110: pppMpNegUntimeout last 0 layer 6
PPPIF-110: CCP Opened
```

IPNCP and CCP have been successfully negotiated. The PPP session has been completely established.

PPPInfo

Description: Displays information about established PPP sessions. Has little practical use other than as a tool for developmental engineering.

Usage: ppinfo *index* [all]

Example:

Syntax element	Description
index	Selects a particular PPP information table.
all	Displays information about embedded structures.

Example:

```
> pppinfo 1
Ncp[LCP]        = B02B396C
Ncp[AUTH]       = B02B39BC
Ncp[CHAP]       = B02B3A0C
Ncp[LQM]        = B02B3A5C
Ncp[IPNCP]      = B02B3AAC
Ncp[BNCP]       = B02B3AFC
Ncp[CCP]        = B02B3B4C
```

```
Ncp[ATNCP]      = B02B3BEC
Ncp[UNKNOWN]    = B02B3C3C
Mode            = async
nOpen pending   = 0
LocalAsyncMap   = 0
RemoteAsyncMap  = 0
Peer Name       = N/A
Rmt Auth State  = RMT_NONE
aibuf           = 0
ipcp            = B03E502C
vJinfo          = 0
localVjInfo     = 0
bncpInfo        = B03E559C
remote          = no
Bad FCS         = a
```

Quit

Description: Exits diagnostic mode.

Usage: **`quit`** .

RadAcct

Description: Displays RADIUS accounting information. The RadAcct command displays very few messages if RADIUS Accounting is functioning correctly. The command is a toggle that alternately enables and disables the diagnostic display.

(For troubleshooting RADIUS-related issues, the RADIF command displays more detailed information.)

Usage: **`radacct`** .

Example:

```
> radacct
RADACCT debug display is ON
```

A user hangs up and a stop record is generated:

```
RADACCT-147:stopRadAcct
```

The following message indicates that there is some load on the network and the sending of a stop record is delayed. This does not necessarily indicate a problem:

```
RADACCT-147:_endRadAcct: STOP was delayed
```

RadIF

Description: Displays RADIUS-related messages. RadIF is a powerful diagnostic command, because it displays RADIUS messages the DSL Terminator receives as well as messages that it sends. Output from RadIF, in conjunction with running your RADIUS daemon in diagnostic mode (using the `-x` option), gives you virtually all the information you need to clarify issues relating to user authentication.

You can also validate the IP port that you have configured (or think you have configured), and the user name that is being sent by the client.

The command is a toggle that alternately enables and disables the diagnostic display.

Usage: **`radif`** .

Example: Following are messages you might see for a successful RADIUS authentication:

```
RADIF: authenticating <8:my_name> with PAP
RADIF: _radiusRequest: id 41, user name <9:my_name>
RADIF: _radiusRequest: challenge len = <0>
```

The RADIUS daemon IP address and authentication port appear:

```
RADIF: _radiusRequest: socket 5 len 89 ipaddr 01010101 port
65534->1645
RADIF: _radCallback
RADIF: _radCallback, buf = B05BBFA0
```

The response is sent back from RADIUS. In this case, the user `my_name` has passed authentication. Following is a list of the most common responses:

```
   1 - Authentication Request
   2 - Positive Acknowledgement
   3 - Rejection
   4 - Accounting Request
   5 - Accounting Response
   7 - Password Change Request
   8 - Password Change Positive Acknowledgement
   9 - Password Change Rejection
   11 - Access Challenge
   29 - Password - next code
   30 - Password New PIN
   31 - Password Terminate Session
   32 - Password Expired
RADIF: _radCallback, authcode = 2
RADIF: Authentication Ack
```

After authenticating a user, the RADIUS daemon sends the attributes from the user profile to the DSL Terminator. The DSL Terminator creates the user's Connection profile from these attributes, and RadIF displays them. For a complete list of attribute numbers, see the *TAOS RADIUS Guide and Reference*.

```
RADIF: attribute 6, len 6, 00 00 00 02
RADIF: attribute 7, len 6, 00 00 00 01
RADIF: attribute 8, len 6, ff ff ff fe
RADIF: attribute 9, len 6, ff ff ff 00
RADIF: attribute 11, len 12, 73 74 64 2e
RADIF: attribute 12, len 6, 00 00 05 dc
RADIF: attribute 10, len 6, 00 00 00 00
RADIF: attribute 13, len 6, 00 00 00 01
RADIF: attribute 244, len 6, 00 00 11 94
RADIF: attribute 169, len 6, 00 00 11 94
RADIF: attribute 170, len 6, 00 00 00 02
```

```
RADIF: attribute 245, len 6, 00 00 00 00
RADIF: attribute 235, len 6, 00 00 00 01
```

A RADIUS Accounting Start packet is sent to the RADIUS Accounting Server (using port 1646):

```
RADIF: _radiusAcctRequest: id 42, user name <9:my_name>
RADIF: _radiusAcctRequest: socket 6 len 82 IP cf9e400b port
1646, ID=42
RADIF: _radCallback
RADIF: _radCallback, buf = B05433C0
RADIF: _radProcAcctRsp: user:<9:my_name>, ID=42
```

Reset

Description: Resets the DSL Terminator, which terminates all active connections and restarts. All users are logged out and the default security level is reactivated. All active WAN lines are temporarily shut down because of the loss of signaling or framing information. As the DSL Terminator boots, it runs its Power-On Self Tests (POST).

Usage: **`reset`** .

Example: To reset the unit:

```
> reset
```

See Also: NVRAM

TRestore

Description: Restores a saved configuration from a TFTP host to Flash memory on the DSL Terminator. You need to manually reboot the DSL Terminator to load the restored configuration from Flash memory into dynamic RAM.

`Usage: trestore` *`name_or_ip_address_of_tftp_server filename`*

Example:

```
> trestore 1.1.1.1 config.txt
restoring configuration from 1.1.1.1:69
file config.txt...
```

TSave

Description: Saves the DSL Terminator configuration that is stored in flash memory to a TFTP server. You need to perform the FSave command if you want to save your currently running configuration. FSave saves the currently running configuration to flash memory.

`Usage: tsave` *`name_or_ip_address_of_tftp_server filename`*

Example:

```
> tsave 1.1.1.1 config.txt
saving configuration to 1.1.1.1:69
file config.txt...
```

Update

Description: Modifies optional functionality of the DSL Terminator. To enable some options, you must obtain a set of hash codes (supplied by an Lucent representative) that will enable the functionality in your DSL Terminator. After each string is entered, the word *complete* appears, indicating that the DSL Terminator accepted the hash code.

If you enter the update command without a text string modifier, the DSL Terminator displays a list of current configuration information.

Usage: update [*text_string*]

Example:

```
> update
Host interfaces: 4
Net interfaces: 4
Port 1 channels: 255
Port 2 channels: 255
Port 3 channels: 255
Port 4 channels: 255
Field features 1: 182
Field features 2: 33
Field features 3: 54
Protocols: 1
> update 5 1023 12321312312312321
```

The following two messages indicate that the text strings were entered incorrectly:

```
update command: invalid arg 3!
update command: disallowed
```

The following message indicates that the DSL Terminator accepted the update string:

```
update command: command complete.
```

WANDisplay

Description: Displays all packets received from or sent to any of the WAN interfaces. Because WANDisplay ouput shows the raw data the DSL Terminator is receiving from and sending to the remote device, the information can be very helpful in PPP negotiation problems.

If you enter the command while traffic through your DSL Terminator is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message `----- data lost -----`, which just means that not all the output can be displayed on the screen.

You might prefer to use the WANDisplay command during a period of low activity. Alternatively, depending on the types of information you need to gather, you might use WANDSess, WANOpen, or WANNext to focus the display.

Usage: wandisplay ***number_of_octets_to display_from_each_packet***

Enter **wandisplay 0** to disable the logging of this information.

Example: Following are several examples of WANDisplay output. Note that the bytes are displayed in hexadecimal format.

```
> wandisplay 24
Display the first 24 bytes of WAN messages
> RECV-272:: 1 octets @ 5E138F74
[0000]: 0D
RECV-272:: 13 octets @ 5E13958C
[0000]: 0A 41 63 63 65 70 74 3A 20 69 6D 61 67
XMIT-276:: 1011 octets @ 2E12D8A4
[0000]: 7E 21 45 00 03 EE 54 2B 40 00 37 06 BA 09 CF 2B
[0010]: 00 86 D0 93 91 90 1A 0A
> wandisplay 0
WAN message display terminated
```

See Also: WANDSess, WANOpening, WANNext

WANDSess

Description: Similar to WANDisplay, but WANDSess displays only incoming and outgoing packets for a specific user. WANDSess is particularly helpful for troubleshooting a DSL Terminator with several simultaneous active connections. The volume of output from commands such as WANDisplay make them not as effective for troubleshooting issues for particular users. WANDSess is a filter to let you focus your troubleshooting.

Even though WANDSess does act as a filter, if you enter the command while traffic through your DSL Terminator is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message `----- data lost -----`, which just means that not all the output can be displayed on the screen. You might prefer to use the WANDSess command during a period of low activity.

Usage: wandsess *user_name_or_profile_name number_of octets_to_display_from each_packet*

Enter `wandsess` *`user_name_or_profile_name`* `0` to disable the logging of this information.

Example:

```
> wandsess gzoller 24
RECV-gzoller:300:: 1 octets @ 3E13403C
[0000]: 7E 21 45 00 00 3E 15 00 00 00 20 7D 31 C2 D2
RECV-gzoller:300:: 15 octets @ 3E133A24
[0000]: D0 7D B3 7D B1 B3 D0 7D B3 90 02 04 03 00 35
XMIT-gzoller:300:: 84 octets @ 3E12D28C
[0000]: 7E 21 45 00 00 4E C4 63 00 00 1C 7D 31 17 5F D0
[0010]: 93 90 02 D0 93 91 B3 00
```

Notice that thedifference in output between WANDSess and WANDisplay is that WANDSess limtis the output to one session and the name of the user is displayed in a message. The data is identical in content, but WANDSess displays no data from any other sessions.

> **wandsess gzoller 0**

See Also: WANDisplay, WANNext, WANOpening

WANNext

Description: Similar to WANDisplay, but WANNext displays only incoming and outgoing packets for the next successfully authenticated user. As with WANDSess, the output is the same as for WANDisplay but is filtered to include only data from a single user.

Even though WANNext asct as an output filter, if you enter the command while traffic through your DSL Terminator is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message `----- data lost -----`, which just means that not all the output can be displayed on the screen. You might prefer to use the WANNext command during a period of low activity.

`Usage: wannext` *`number_of_octets_to_display_from_each_packet`*

Enter `WANNext 0` to disable the logging of this information.

WANOpening

Description: Similar to WANDisplay, but WANOpening displays only the opening incoming and outgoing packets for all users during the establishment of their PPP sessions. This command is particularly helpful if you are troubleshooting connection problems in which users seem to connect to the DSL Terminator but are disconnected within a few seconds. Again, the output from WANOpening is very similar to WANDisplay but WANOpening displays packets for sessions only until the connection has been completely negotiated.

Even though WANOpening limits the output seen on the screen, if you enter the command while traffic through your DSL Terminator is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message `----- data lost -----`, which just means that not all the output can be displayed on the screen. You might prefer to use the WANOpening command during a period of low activity.

`Usage: wanopening` *`number_of_octets_to_display_from_each_packet`*

Enter `WANOpening 0` to disable the logging of this information.

WANToggle

Description: Displays messages from the WAN drivers on the DSL Terminator, including the state of calls that have been processed by the DSL Terminator's calling routines but not yet sent to the Ethernet drivers.

If you enter the command while traffic through your DSL Terminator is heavy, the resulting amount of output can make it tedious to find the information you are looking for. The screen might even display the message `----- data lost -----`, which just means that not all the output can be displayed on the screen. You might prefer to use the WANToggle command during a period of low activity.

The command is a toggle that alternately enables and disables the diagnostic display.

Usage: `wantoggle`.

Example: Typical output produced by a modem call into the DSL Terminator is similar to that found below. After the incoming call is determined to be an analog call, a modem is directed to answer it.

```
WAN-389: wanOpenAnswer
WAN-389: modem redirected back to wan
WAN-389: Startup frame received
WAN-389: Detected unknown message
WAN-389: Detected ASYNC PPP message
WAN-389: wanRegisterData, I/F 58
```

The next two messages appear when the call is cleared. The second message does not indicate a problem. It appears because the modem clears the call a split second before the software releases its resources. The software does a check on the modem, which has already been released.

```
WAN-389: wanCloseSession, I/F 58
WAN-??: no modem assoc w WanInfo
```

WDDialout

Description: Displays the specific packet that caused the DSL Terminator to dial out. The command is particularly helpful if the DSL Terminator is dialing out when it should not. You can use `WDDialout` information to design a filter to keep the DSL Terminator from dialing out because of a particular packet.

The command is a toggle that alternately enables and disables the diagnostic display.

Usage: **`wddialout`**.

Example: The following message includes a date/time stamp, the phone number being dialed, and the packet that caused the DSL Terminator to dial out:

```
Date: 01/01/1990.     Time: 00:51:56
Cause an attempt to place call to 18185551234
WD_DIALOUT_DISP: chunk D7BA6 type OLD-STYLE-PADDED.
: 60 octets @ F3050
[0000]: 09 00 07 ff ff ff 00 05 02 e8 14 0d 00 24 aa aa
[0010]: 03 00 00 00 80 f3 00 01 80 9b 06 04 00 01 00 05
[0020]: 02 e8 14 0d 00 ff 00 f7 00 00 00 00 00 00 00 ff
[0030]: 8e 01 00 00 00 00 00 00 00 00 00 00
> wddialout
WANDATA dialout display is OFF
```

PPP decoding primer

Many of the diagnostic commands display raw data. This section to assists you in decoding PPP, MP, MP+ and BACP negotiations. The negotiations can be logged with the PPPDump,

WANDisplay, WANDSess, WANNext, or WANOpen diagnostic commands. For more detailed information than this appendix provides, see specific RFCs. A partial list of pertinent RFCs appears at the end of this appendix.

Breaking down the raw data

An important concept to keep in mind is that each device negotiates PPP independently, so the options might be identical for each direction of the session. During PPP negotiation, frame formats in the various protocols are very similar. They share the following characteristics:

- `FF 03` which indicates a PPP frame
- A two-byte Protocol Identifier
- A one-byte Packet Format ID number
- A one-byte ID number
- A two-byte length
- Options for the protocol

Following are the most common protocols you will see in Lucent diagnostic traces:

Identifier	Description
C0 21	Link Control Protocol (LCP)
C0 23	Password Authentication Protocol (PAP)
C2 23	Challenge Handshake Authentication Protocol (CHAP)
80 21	Internet Protocol (IP)
80 29	Appletalk (Appletalk is not applicable to DSL Terminator)
80 2B	Novell's Internetwork Packet Exchange (IPX) (IPX is not applicable to the DSL Terminator.)
80 31	Bridging PDU
80 FD	Compression Control Protocol (CCP)

Following are the packet formats:

Packet Format ID	Description
01	Configure Request
02	Configure Acknowledgment
03	Configure Non-Acknowledgment
04	Configure Reject
05	Terminate Request

Packet Format ID	Description
06	Terminate Acknowledgment
07	Code Reject
08	Protocol Reject
09	Echo Request
0A	Echo Reply
0B	Discard Request

Note: If a packet received from the WAN fails the Cyclic Redundancy Check (CRC), the display is similar to the following, where RBAD denotes Received BAD:

```
RBAD-27:: 8712 octets @ 26CFE8
[0000]: fe dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd
[0010]: dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd
[0020]: dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd
[0030]: dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd dd
```

Annotated Traces

Following are sample traces you can use as guides to help you decode other traces.

Example of a PPP connection attempt

LCP Configure Request—MP+, MRU of 1524, MRRU of 1524 and End Point Discriminator using the device's MAC address:

```
XMIT-3:: 29 octets @ 2C2E94
[0000]: ff 03 c0 21 01 01 00 19 00 04 00 00 01 04 05 f4
[0010]: 11 04 05 f4 13 09 03 00 c0 7b 4c e0 4c
```

Following is a second LCP Configure Request from the same device. Everything in the packet is identical to the previous packet, except the ID number has incremented from 01 to 02:

```
XMIT-3:: 29 octets @ 2C2E94
[0000]: ff 03 c0 21 01 02 00 19 00 04 00 00 01 04 05 f4
[0010]: 11 04 05 f4 13 09 03 00 c0 7b 4c e0 4c
```

LCP Configure Request—CHAP authentication, Magic number

```
RECV-3:: 19 octets @ 2BEB8C
[0000]: ff 03 c0 21 01 60 00 0f 03 05 c2 23 05 05 06 4e
[0010]: 36 c9 05
```

LCP Configure Acknowledgment—The device in the following trace will be authenticated with CHAP. The Magic number is also acknowledged:

```
XMIT-3:: 19 octets @ 2C2E94
[0000]: ff 03 c0 21 02 60 00 0f 03 05 c2 23 05 05 06 4e
[0010]: 36 c9 05
```

LCP Configure Reject—MP+, MRU of 1524, MRRU of 1524 and End Point Discriminator. This rejection shows two things. First, the remote side does not support MP+ or MP, since MP+ and the MRRU were rejected. This will have to be a PPP connection. Second, since the MRU of 1524 was rejected, the default of 1500 is assumed. There must be an MRU, so a rejection of a given value only calls for use of the default value.

After the trace, the device will need to transmit another LCP Configure Request, removing all the rejected options:

```
RECV-3:: 29 octets @ 2BF1A4
[0000]: ff 03 c0 21 04 02 00 19 00 04 00 00 01 04 05 f4
[0010]: 11 04 05 f4 13 09 03 00 c0 7b 4c e0 4c
```

LCP Configure Request—Note that all values that were previously rejected are no longer in the packet:

```
XMIT-3:: 8 octets @ 2C2E94
[0000]: ff 03 c0 21 01 04 00 04
```

LCP Configure Acknowledgment:

```
RECV-3:: 8 octets @ 2BF7BC
[0000]: ff 03 c0 21 02 04 00 04
```

At this point, since both sides have transmitted LCP Configure Acknowledgments, LCP is up and the negotiation moves to the authentication phase. The device receives a CHAP challenge from the remote end:

```
RECV-3:: 21 octets @ 2BFDD4
[0000]: ff 03 c2 23 01 01 00 11 04 4e 36 c9 5e 63 6c 63
[0010]: 72 34 30 30 30
```

The device transmits its encrypted user name and password:

```
XMIT-3:: 36 octets @ 2C2E94
[0000]: ff 03 c2 23 02 01 00 20 10 49 b8 e8 54 76 3c 4a
[0010]: 6f 30 16 4e c0 6b 38 ed b9 4c 26 48 5f 53 65 61
[0020]: 74 74 6c 65
```

The remote device sends a CHAP Acknowledgment:

```
RECV-3:: 8 octets @ 2C03EC
[0000]: ff 03 c2 23 03 01 00 04
```

At this point, the negotiation moves from authentication to negotiation of Network Control Protocols (NCPs). Lucent supports Bridging Control Protocol (BCP), IPCP, and ATCP.

IPCP Configure Request—Van Jacobsen Header Compression, IP address of 1.1.1.1:

```
RECV-3:: 20 octets @ 2C0A04
[0000]: ff 03 80 21 01 e3 00 10 02 06 00 2d 0f 00 03 06
[0010]: 01 01 01 01
```

BCP Configure Request:

```
RECV-3:: 8 octets @ 2C101C
[0000]: ff 03 80 31 01 55 00 04
```

IPCP Configure Request—IP address of 2.2.2.2:

```
XMIT-3:: 14 octets @ 2C2E94
[0000]: ff 03 80 21 01 01 00 0a 03 06 02 02 02 02
```

IPCP Configure Reject—Van Jacobsen Header Compression. The remote device should send another IPCP Configure Request and remove the request to perform VJ Header Compression:

```
XMIT-3:: 14 octets @ 2C2E94
[0000]: ff 03 80 21 04 e3 00 0a 02 06 00 2d 0f 00
```

BCP - Protocol Reject. The local device is not configured to support bridging:

```
XMIT-3:: 8 octets @ 2C2E94
[0000]: ff 03 80 31 08 55 00 04
```

IPCP Configure Acknowledgment:

```
RECV-3:: 14 octets @ 2C1634
[0000]: ff 03 80 21 02 01 00 0a 03 06 01 01 01 01
```

IPCP Configure Request—Note that VJ Header Compression is not requested this time:

```
RECV-3:: 14 octets @ 2C1C4C
[0000]: ff 03 80 21 01 e4 00 0a 03 06 02 02 02 02
```

IPCP Configure Acknowledgment:

```
XMIT-3:: 14 octets @ 2C2E94
[0000]: ff 03 80 21 02 e4 00 0a 03 06 01 01 01 01
```

At this point, a PPP connection has been successfully negotiated. The caller was successfully authenticated by means of CHAP, and IPCP was the only successfully configured NCP. Bridging will not be supported during this session.

Following are two packets used in determining link quality:

LCP Echo Request packet:

```
RECV-3:: 16 octets @ 2BEB8C
[0000]: ff 03 c0 21 09 01 00 0c 4e 36 c9 05 00 00 00 00
```

LCP Echo Response:

```
XMIT-3:: 16 octets @ 2C2E94
[0000]: ff 03 c0 21 0a 01 00 0c 00 00 00 00 00 00 00 00
```

Example of MP+ call negotiation

LCP Configuration Request—MP+, MRU of 1524, MRRU of 1524, End Point Discriminator using the device's MAC address:

```
XMIT-31:: 29 octets @ D803C
[0000]: ff 03 c0 21 01 01 00 19 00 04 00 00 01 04 05 f4
[0010]: 11 04 05 f4 13 09 03 00 c0 7b 5c d3 71
```

LCP Configure Request—MP+, MRU of 1524, PAP authentication is required. MRRU of 1524, End Point Discriminator using the device's MAC address:

```
RECV-31:: 33 octets @ D4FBC
[0000]: ff 03 c0 21 01 01 00 1d 00 04 00 00 01 04 05 f4
[0010]: 03 04 c0 23 11 04 05 f4 13 09 03 00 c0 7b 53 f0
[0020]: 7a
```

LCP Configuration Acknowledgment:

```
RECV-31:: 29 octets @ D55CC
[0000]: ff 03 c0 21 02 01 00 19 00 04 00 00 01 04 05 f4
[0010]: 11 04 05 f4 13 09 03 00 c0 7b 5c d3 71
```

LCP Configuration Acknowledgment:

```
XMIT-31:: 33 octets @ D803C
[0000]: ff 03 c0 21 02 01 00 1d 00 04 00 00 01 04 05 f4
[0010]: 03 04 c0 23 11 04 05 f4 13 09 03 00 c0 7b 53 f0
[0020]: 7a
```

At this point, LCP is up. Next is the authentication phase. The local device agreed to PAP authentication, so it should transmit its user name and password. Note that they are not encrypted and can be decoded very easily.

PAP Authentication Request—User name is shown in hexadecimal and must be converted to ASCII. User name is 0x6a 0x73 0x6d 0x69 0x74 0x68 (jsmith) and password is 0x72 0x65 0x64 (red):

```
XMIT-31:: 20 octets @ D803C
[0000]: ff 03 c0 23 01 01 00 10 06 6a 73 6d 69 74 68 03 72
[0010]: 65 64
```

PAP Authentication Acknowledgment:

```
RECV-31:: 9 octets @ D5BDC
[0000]: ff 03 c0 23 02 01 00 05 00
```

Authentication is successful. Final negotiation determines protocols to be supported over the link.

Note: MP+ was negotiated, and both devices begin sending MP+ packets from this point. The data portion of the packet is identical to PPP, but there is an eight-byte MP+ header instead of the two-byte PPP header:

In the following packet, `00 3d` is the designation for a Multilink packet. The fifth byte designates whether this packet is fragmented. The sixth, seventh, and eighth bytes are the sequence number, which increments by one for each packet sent or received. Bytes nine through eleven, 80 31 01, designate as a BCP Configure Request received from the remote device:

```
RECV-31:: 20 octets @ D61EC
[0000]: ff 03 00 3d c0 00 00 00 80 31 01 01 00 0a 03 03
[0010]: 01 07 03 00
```

BCP Configure Request sent from this device:

```
XMIT-31:: 20 octets @ D803C
[0000]: ff 03 00 3d c0 00 00 00 80 31 01 01 00 0a 03 03
[0010]: 01 07 03 00
```

BCP Configure Acknowledgment:

```
XMIT-31:: 20 octets @ D864C
[0000]: ff 03 00 3d c0 00 00 01 80 31 02 01 00 0a 03 03
[0010]: 01 07 03 00
```

BCP Configure Acknowledgment:

```
RECV-31:: 20 octets @ D67FC
[0000]: ff 03 00 3d c0 00 00 01 80 31 02 01 00 0a 03 03
[0010]: 01 07 03 00
```

BCP is up and the session begins sending bridged traffic. No routed protocols were negotiated.

The following packets are sent as part of the MP+ protocol. They are sent at 1-second intervals. The packets are used by each unit to validate the existence of the link. This validation gives the devices a secure way to determine whether the link is still up, even if there is no data traffic passing between the devices.

```
RECV-31:: 8 octets @ D5BDC
[0000]: ff 03 00 3d c0 00 00 05
XMIT-31:: 8 octets @ D803C
[0000]: ff 03 00 3d c0 00 00 04
RECV-31:: 8 octets @ D61EC
[0000]: ff 03 00 3d c0 00 00 06
XMIT-31:: 8 octets @ D803C
[0000]: ff 03 00 3d c0 00 00 05
```

Relevant RFCs

The following RFCs provide more detail about the protocols used in Lucent diagnostic traces.

Identifier	Title
RFC 1638	PPP Bridging Control Protocol (BCP)
RFC 1661	Point-to-Point Protocol (PPP)
RFC 1934	Ascend's Multilink Protocol Plus (MP+)
RFC 1962	PPP Compression Control Protocol (CCP)
RFC 1974	PPP Stac LZS Compression Protocol
RFC 1989	PPP Link Quality Monitoring
RFC 1990	PPP Multilink Protocol (MP)
RFC 1994	PPP Challenge Handshake Authentication Protocol

Upgrading System Software

C

Caution: Periodically the procedure for uploading new software to DSL Terminator units changes significantly. Carefully read the new software loading procedures explained in this section before upgrading your system.

This appendix explains how to change your system software by either upgrading or downgrading it. Before you upgrade or downgrade your software, review the related terms and definitions in the following list and review the guidelines for upgrading and downgrading in the sections “Guidelines for upgrading system software” on page C-1 and “Downgrading system software” on page C-7

For the names of all the software builds and the features they provide, see `fttp://ftp.ascend.com/pub/Software-Releases/Terminator/` on the FTP server. .

Guidelines for upgrading system software

Caution: Before upgrading, consider the following very important guidelines:

- Use TFTP to upgrade if possible. TFTP is more reliable and saves the DSL Terminator unit configuration when you upgrade.
- If you are using TFTP to upgrade your software, use the `fsave` command immediately after executing the `tload` command. Failure to do so might cause your DSL Terminator to lose its configuration.
- If possible, always stay with the same build of software when you upgrade. If you load a different version, your DSL Terminator may lose its configuration. If this happens, you must restore your configuration from a backup.

Preparing to upgrade your software

Make sure you perform all the tasks explained in Table C-1 before upgrading your software.

Table C-1. Before upgrading

Task	Description
If necessary, activate a Security Profile that allows for field upgrade.	If you are not sure how, see the section about Security Profiles in your documentation.
Record all of the passwords you want to retain, and save your unit's current configuration to your computer's hard disk.	For security reasons, passwords are not written to configuration files created through the serial console. A configuration file created using the `Tsave` command, however, *does* contain the system passwords. You can restore the `Tsave` configuration file using the serial console. If you chose to save your configuration using the serial console, you have to restore your passwords manually. Restoring passwords is explained in "Restoring passwords" on page C-6.
Obtain the correct file, either by downloading it from the FTP server or by requesting it from Lucent technical support.	To ensure that you load the correct software binary, check the load currently installed on your unit. To do so: **1** Tab over to the 00-100 Sys Options window. **2** Press Enter to open the Sys Options menu. **3** Using the Down-Arrow key (or Ctrl- N), scroll down until you see a line similar to the following: `Load: tl.dm2` **4** When upgrading, obtain the file with same name from the Ascend FTP site. If your unit does not display the current load or you are unsure about which load to use, contact technical support.
If you are using TFTP, make sure you load the correct binaries into the TFTP home directory on the TFTP server.	TFTP is the preferred method of upgrading your unit.
If you are using the serial port, make sure you have a reliable terminal emulation program, such as Procomm Plus.	Upgrading through the serial port is generally not recommended. If you use a Windows-based terminal emulator such as Windows Terminal or HyperTerminal, disable any screen savers or other programs or applications that could interrupt the file transfer. Failure to do so might cause the software upload to halt, and can render the DSL Terminator unusable.

Upgrading system software

To upgrade system software with a standard load you can use either the serial port or TFTP. TFTP is the recommended method because it preserves your DSL Terminator unit's configuration. If you want to use the serial port to upgrade, see "Using the serial port to upgrade" on page C-3.

Using TFTP to upgrade

To upgrade using TFTP, you must enter a few commands in the correct sequence. If you do not enter them in the correct sequence, you could lose the DSL Terminator unit's configuration.

1. Obtain the software version you want to upgrade to and place it in the TFTP server home directory.
2. From the DSL Terminator unit's VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

   `Esc [ Esc =`

   Or, press Ctrl-D to invoke the DO menu and select D=Diagnostics.
3. At the > prompt, use the `Tsave` command to save your configuration. For example, the following command restores the configuration named `router1.cfg` from the TFTP home directory of the server named `tftp-server`. The file must exist and be readable.

   `> tsave -a tftp-server router1.cfg`

   Normally, TFTP upgrades save the configuration. `Tsave` is a precaution.

Caution: The file you save with the `Tsave` command contains all the passwords in clear text. You should move this file from the TFTP directory to a secure location after the upgrade procedure is complete.

4. Enter the following command:

   `tloadcode` ***`hostname filename`***

   replace ***`hostname`*** with the name or IP address of your TFTP server, and ***`filename`*** with the name of the system software on the server (relative to the TFTP home directory).

   For example, the following command loads `t.m40` into flash from the machine named `tftp-server`:

   `tloadcode tftp-server tl.dm2`

Caution: You must use the `Fsave` command immediately after executing the `Tload` command. Failure to do so can cause your DSL Terminator to lose its configuration.

5. Enter the following command to save your configuration to flash memory:

   > **`fsave`**
6. Enter the following command:

   > **`nvramclear`**

   After the DSL Terminator clears NVRAM memory, it automatically resets.

This completes the upgrade.

Using the serial port to upgrade

Caution: Uploading system software via the serial console overwrites all existing profiles. Save your current profiles settings to your hard disk before you begin upgrading system software. After the upgrade, restore your profiles from the backup file you created. The backup file is readable text, so you can reenter the settings through the DSL Terminator unit's user interface. To avoid having existing profiles overwritten, use TFTP to upgrade your unit.

Upgrading through the serial port consists of the following general steps:

- Saving your configuration
- Uploading the software
- Restoring the configuration

Before you begin

Before upgrading your system through the serial port, make sure you have the following equipment and software:

- An IBM compatible PC or Macintosh with a serial port capable of connecting to the DSL Terminator unit's Console port.
- A straight-through serial cable.
- Data communications software for your PC or Mac with XModem CRC/1K support (for example, Procomm Plus, HyperTerminal for PCs, or ZTerm for the Mac).

Caution: If you use a Windows-based terminal emulator such as Windows Terminal or HyperTerminal, disable any screen savers or other programs or applications that could interrupt the file transfer. Failure to do so might cause the software upload to halt, and can render the DSL Terminator unusable.

Saving your configuration

Before you start, verify that your terminal emulation program has a disk capture feature. Disk capture allows your emulator to capture to disk the ASCII characters it receives at its serial port. You must also verify that the data rate of your terminal emulation program is set to the same rate as the Term Rate parameter in the System Profile (Sys Config menu).

You can cancel the backup process at any time by pressing Ctrl-C.

To save theDSL Terminator configuration (except passwords) to disk:

1 Open the Sys Diag menu.

2 Select Save Config, and press Enter.
The following message appears:
`Ready to download - type any key to start....`

3 Turn on the Capture feature of your communications program, and supply a filename for the saved profiles. (Consult the documentation for your communications program if you have any questions about how to turn on the Capture feature.)

4 Press any key to start saving your configured profiles.
Rows of configuration information appear on the screen as the configuration file is downloaded to your hard disk. When the file has been saved, your communications program displays a message indicating the download is complete.

5 Turn off the Capture feature of your communications program.

6 Print a copy of your configured profiles for later reference.

Examine the saved configuration file. Notice that some of the lines begin with `START=` and other lines begin with `END=`. A pair of these START/STOP lines and the block of data between them constitute a profile. If a parameter in a profile is set to its default value, it does not appear.

In fact, you can have profiles with all parameters at their defaults, in which case the corresponding START/STOP blocks are empty. Make sure that no extra lines of text or characters either before `START=` or after `END=`. If there are, delete them. They could cause problems when you try to upload the file to the DSL Terminator.

Uploading the software

To upload the software:

1. Type the following four-key sequence in rapid succession by pressing each key in the sequence shown, one after the other, as quickly as possible:

   `Esc [ Esc -`

   (Press the Escape key, the Left Bracket key, the Escape key, and the Minus key, in that order, in rapid succession.) The following string of Xmodem control characters appears:

   `CKCKCKCK`

   If you do not see these characters, you probably did not press the four-key sequence quickly enough. Try again. Most people use both hands and keep one finger on the Escape key.

2. Use the Xmodem file-transfer protocol to send the system file to the DSL Terminator.

   Your communications program normally takes anywhere from 5 to 15 minutes to send the file to your DSL Terminator. The time displayed on the screen does not represent real time. Do not worry if your communication program displays several “bad batch” messages. This is normal.

After the upload, the DSL Terminator resets. Upon completion of the self-test, the DSL Terminator unit’s initial menu appears in the Edit window with all parameters set to default values. This completes the upgrade.

If the upload fails during the transfer, try downloading another copy of the binary image from the Lucent FTP server and reloading the code to the DSL Terminator. If you still have problems, contact Lucent technical support for assistance.

Restoring the configuration

Under certain circumstances, the serial-port method might not completely restore your configuration. For best results, therefore, verify that your configuration was properly restored every time you use this method. If you have many profiles and passwords, consider using TFTP to upgrade your software. (See “Using TFTP to upgrade” on page C-3.)

To restore the configuration, you must have administrative privileges that include Field Service (such as the Full Access Profile, for example). You use the `Restore Cfg` command to restore a full configuration that you saved by using the `Save Cfg` command, or to upload more specific configuration information obtained from Lucent (for example, a single filter stored in a special configuration file).

To load configuration information through the serial port, perform the following steps:

1. From the DSL Terminator unit’s VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

   `Esc [ Esc =`

   Or, press Ctrl-D to invoke the DO menu, and select D=Diagnostics.

2. At the `>` prompt, enter the `Fclear` command:

```
> fclear
```

3 At the > prompt, enter the `NVRAMClear` command:

```
> nvramclear
```

This causes the system to reset. When it comes back up, proceed with restoring your configuration.

4 Enter **`quit`** to exit the Diagnostic interface.

5 Open the Sys Diag menu.

6 Select `Restore Cfg`, and press Enter.

The following message appears:

```
Waiting for upload data...
```

7 Use the Send ASCII File feature of the communications software to send the configuration file to the unit. (If you have any questions about how to send an ASCII file, consult the documentation for your communications program.)

When the restore has been completed, the following message appears:

```
Restore complete - type any key to return to menu
```

8 Press any key to return to the configuration menus.

9 Reset the DSL Terminator, by selecting System > Sys Diag > Sys Reset and confirming the reset.

Restoring passwords

For security, passwords are not written to configuration files created through the serial console. A configuration file created using the `Tsave` command, however, *does* contain the system passwords. You can restore the `Tsave` configuration file using the serial console.

After upgrading you may have to reenter all the passwords on your system. If you edit your saved configuration file, however, and enter passwords in the appropriate fields (by replacing the word *SECURE* in each instance), these passwords will be restored. But note that if you do choose to edit your configuration file, you must save it as text only or you will not be able to load it into your unit.

If you restored a complete configuration, the passwords used in your Security profiles have been wiped out. To reset them:

1 Press Ctrl-D to invoke the DO menu, select `Password`, and choose the Full Access profile.

2 When you are prompted to enter the password, press Enter (the null password).

After you have restored your privileges by entering the null password, immediately open the Connection profiles, Security profiles, and Ethernet profile (Mod Config menu), and reset the passwords to their previous values.

Upgrade system messages

Table C-2 explains the messages that can appear during your upgrade.

Table C-2. System software messages

Message	Explanation
`This load appears not to support your network interface.` `Download aborted. Use 'tloadcode -f' to force.`	Indicates you are attempting to load a version of code intended for a different network interface (for example, loading MAX 6000 T1 software onto a MAX 6000 E1 unit).
`This load appears to be for another platform.` `Download aborted. Use 'tloadcode -f' to force.`	Indicates you are attempting to load a version of code onto a platform for which it is not intended (for example, loading MAX 6000 software onto a DSL Terminator). This is not recommended.

Downgrading system software

The DSL Terminator expects a specific organization of the parameters in a configuration file. When you upgrade, you *can* restore a configuration that was saved on an older release. The DSL Terminator enters default values for parameters if the unit supports a parameter that is not included in the configuration file.

When you downgrade to older versions of software, the configuration might not upload completely, because older software does not support the parameters that might be in configuration files from newer releases.

You must upload a configuration that was saved from the same version of software to make sure that the unit receives a complete configuration. If you upload a configuration from a newer version of software, you must check all parameter values to verify they are configured accurately.

If you are downgrading system software, make sure that you have a configuration saved from a DSL Terminator running with the older software and that you have console access to the unit. Then, proceed as follows:

1. Use TFTP to load the system software.
2. Enter **`FCLEAR`** to clear the unit's flash memory.
3. Enter **`NVRAMCLEAR`** to clear the unit's main configuration and reset the DSL Terminator.
   The DSL Terminator restarts and loads the older version of system software.
4. When the DSL Terminator is up, manually enter basic information, including IP address, subnet mask, and default gateway to the Ethernet interface.
   After entering you must be able to use Telnet to access the DSL Terminator.
5. From the DSL Terminator unit's VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

   `Esc [ Esc =`

   Or, press Ctrl-D to invoke the DO menu and select D=Diagnostics.

6 At the > prompt, use the `TRestore` command to restore the configuration. For example, the following command restores the configuration named `router1.cfg` from the TFTP home directory of the server named `tftp-server`. The file must exist and be readable.

```
> trestore tftp-server router1.cfg
```

7 At the > prompt, enter **`Exit`** to return to the VT100 interface.

Index

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X