Lucent Technologies
Bell Labs Innovations

DSL Terminator™

Reference

Part Number: 7820-0774-001
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

About This Reference

What is in this reference

This reference contains parameters in alphabetical order. The index can help you to dinf additional information.

Note: This manual describes the full set of features for units running software version 7.1.0. Some features might not be available with earlier versions or specialty loads of the software.

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

What you should know

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

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 monospace 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.

Convention	Meaning
|	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.
 **Warning:**	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment, or physical injury.
 **Warning:**	Warns that a failure to take appropriate safety precautions could result in electrical shock.

Documentation set

The documentation set consists of the following manuals:

- *DSL Terminator Network Configuration Guide*
- *DSL Terminator Administration Guide*
- *DSL Terminator Reference (this manual)*
- *DSL Terminator Hardware Installation Guide*
- *TAOS RADIUS Guide and Reference*
- *TAOS Glossary*
- *Access Networks Safety and Compliance Guide*

Related publications

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

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

DO Commands and Terminal Server Commands

1

This DSL Terminator interface includes a number of shortcut commands to control the DSL Terminator or to switch to another of its interfaces. These are called DO commands. The interface also includes an number of commands to control the terminal server. These are called T-Server commands. This chapter describes both types of commands.

Other types of commands, such as the debug commands, are covered in the *DSL Terminator Adminstration Guide*.

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
 1=Dial
 P=Password
 S=Save
 E=Termserv
 D=Diagnostics
```

Using DO commands

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.

DO command reference in alphabetic order

DO commands provide shortcuts to control the DSL Terminator or to switch to another of its interfaces. This section lists the DO commands in alphabetic order and describes them in detail.

Close Telnet (DO C)

Description: Closes the current Telnet session.

Usage: You must be running a Telnet session from the DSL Terminator's terminal-server interface.

Diagnostics (DO D)

Description: Invokes diagnostics mode.

Usage: 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
```

See Also: The diagnostics commands are described in the *DSL Terminator Adminstration Guide*.

Esc (DO 0)

The DO ESC command exits the DO menu.

Load (DO L)

Description: Loads a saved or edited profile and overwrites the values of the current profile.

Usage: Allows you to replace an entire profile in a few keystrokes.

Example: If you have saved a profile named Memphis in the Directory location 21-102 and your screen currently displays the following lines:

```
21-100 Directory
  21-1 Factory
  21-101 Tucson
 >21-102 Memphis
```

If you execute DO Load, you see:

```
Load profile...?
  0=Esc (Don't load)
  1=Load profile 102
```

If you choose the first option by pressing 0 (zero), the DSL Terminator aborts the load operation. If you choose the second option by pressing 1, the following status window appears:

```
Status #116
  profile loaded
  as current profile
```

The Directory menu shows the results of the load operation:

```
21-100 Directory
  21-1** Memphis
  21-101 Tucson
 >21-102 Memphis
```

The DO Load command is not available if you are not logged in with operational privileges. For more information, see the Operations parameter on page 2-106.

Menu Save (DO M)

Description: Saves the entire current VT100 interface layout. The current layout replaces the default layout.

Dependencies:

- The DO Menu Save command appears only if the cursor is in front of the Sys Config menu.
- The command always places Sys Config in the default Edit display. (To change the default Edit display, you must configure the Edit parameter in the System profile after using the DO Menu Save command.)

For related information, see the Edit parameter on page 2-52.

Password (DO P)

Description: Enables you to log into the DSL Terminator.

Permission level: .

Usage: 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.

Dependencies: 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 parameter on page 2-21 and the Idle Logout parameter on page 2-74.

Save (DO S)

The DO Save command saves the current parameter values in a specified profile.

Keep in mind the following additional information:

- If a profile is protected by a Security profile, you might not be able to overwrite it.
- Save does not appear if you are not logged in with operational privileges.

For more information, see the Operations parameter in the *DSL Terminator Reference Guide.*

Termserv (DO E)

Description: Invokes the terminal-server command-line interface.

Permission level: The user must have sufficient privileges in the active Security profile.

Usage: 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 Guide*. To exit terminal-server mode and return to the VT100 interface, enter the Quit command:

```
ascend% quit
```

Terminal-server command-line interface

The terminal-server command-line interface can provide 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 the *DSL Terminator Adminstration Guide*). 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 in rapid succession:

`Esc [ Esc 0` (Escape key, left bracket, Escape key, zero)

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 <*s*>
`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 <hostname>
`traceroute`	Trace route to host. Type 'traceroute -?' for help

For details about each of the commands, see *DSL Terminator Adminstration Guide*

Commands for the terminal-servers

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

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

Description: Initiates a login session to a remote host.

Usage: **`telnet`** `[-a|-b|-t]` ***`<hostname`*** `[`***`port-number`***`]`**`>`**

Keyword	Description
`-a``|` **`-b`**`|` **`-t`**	Optional mode arguments specifying ASCII, Binary, or Transparent mode, respectively. When entered, overrides the setting of the current Telnet Mode argument. • ASCII mode: the DSL Terminator uses standard 7-bit mode. • 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. • Transparent mode: either of the other modes can be used without specifying the mode.
`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`	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.

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

```
ascend% telnet myhost
```

Several options in the Ethernet > Mod Config > TServ Options subprofile also affect Telnet; for example, if you set `Def Telnet = 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 1-7. 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, hold down the Control key and type a right bracket (`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.

Command	Description
`Ctrl]` (hold down the Control key and type a right bracket)	Displays the Telnet prompt while logged in to a host
`telnet>` **`?`**	Displays information about Telnet session commands.
`telnet>` **`Help`**	Displays information about Telnet session commands.
`telnet>` **`open myhost`**	Opens a Telnet connection after invoking Telnet.
`telnet>` **`send susp`**	Sends standard Telnet commands such as `Are You There` or `Suspend Process`
`telnet>` **`send ?`**	Displays a list of Send commands and their syntax.
`telnet>` **`set eof ^D`**	Specifies special characters for use during the Telnet session.
`telnet>` **`set all`**	Displays current settings.
`telnet>` **`set ?`**	Displays a list of Set command
`telnet>` **`close`**	Quits the Telnet session and closes the connection.

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:

Keyword	Description
-echar	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 you 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 you 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 TCP session starts running initially, 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 an unencumbred TCP connection fails, the DSL Terminator returns one of the following error messages:

Error message	**Explanation**
`Cannot open session:` *`<hostname> <port-number>`*	You entered an invalid or unknown value for *`hostname`* you entered an invalid value for *`port-number`* 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: host reset`	The destination network is unreachable

Administrative commands

The following commands are useful for system administration:

`remote`	start a mremote management session at<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 *DSL Terminator Administration Guide*).

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:

Table 1-1. Errors in Remote Session Management

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.

Table 1-1. Errors in Remote Session Management (continued)

Message	Explanation
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. For details, see the *Network Configuration Guide* for your DSL Terminator.

Show

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

Parameter Reference

2

A DSL Terminator unit supports a variety of software loads that are customized to particular purposes. The installed software might not support all of the parameters described here. For example, Network Address Translation (NAT) and Internet Packet eXchange (IPX) are referred to in some cases, but neither of these protocols is supported by the DSL Terminator.

Numeric

2nd Adrs

Description: Assigns a second IP address to the Ethernet interface. The 2nd Adrs value gives the DSL Terminator unit a logical interface on two networks or two subnets on the same backbone, a feature called *dual IP.*

Usage: Specify a valid IP address on the remote subnet. The default value is 0.0.0.0/0.

Example: `2nd Adrs=10.65.212.56/24`

Location: Ethernet > Mod Config > Ether Options

See Also: IP Adrs

A

Acct

Description: Specifies the type of accounting service to use for incoming and outgoing bridging or routing calls.

Usage: Specify one of the following values:

- `None` (the default) specifies that no accounting takes place.
- `RADIUS` enables RADIUS accounting.
- `TACACS+` enables TACACS+ accounting.

Example: `Acct = none`

Dependencies: RADIUS accounting is disabled if you set Auth=RADIUS/LOGOUT. When you enable accounting by means of RADIUS or TACACS+, you must specify the address of the server by means of the Acct Host parameter.

Location: Ethernet > Mod Config > Accounting

See Also: Acct Host #N, Auth

Acct Checkpoint

Description: Specifies, in minutes, the interval at which RADIUS accounting Checkpoint records should be sent for all users. The Checkpoint message contains the same attributes as the Stop message, except that the value for Acct-Status-Type is 3 (Checkpoint).

Usage: Specify a number from 0 to 60. The default setting is 0 (zero), which disables the Checkpoint feature.

Example: `Acct checkpoint = 50`

Dependencies: The Acct Checkpoint parameter does not apply (Acct Checkpoint=N/A) if RADIUS accounting is not in use.

Location: Ethernet > Mod Config > Accounting

See Also: Acct

Acct Compat Mode

Description: Enables or disables Vendor-Specific Attribute (VSA) compatibility mode when the DSL Terminator unit is using RADIUS for accounting purposes.

Usage: Specify one of the following settings:

- Old (the default) specifies that the DSL Terminator unit does not send the Vendor-Specific attribute to the RADIUS server and does not recognize the Vendor-Specific attribute if the server sends it.

- Vendor-Specific specifies that the DSL Terminator unit uses the Vendor-Specific attribute to encapsulate Lucent vendor attributes, and uses the RFC-defined User-Password encryption algorithm as well.

Example: `Acct compat mode = old`

Location: Ethernet > Mod Config > Accounting

See Also: Auth Compat Mode, Compat Mode

Acct Host

Description: Specifies the IP address of a connection-specific accounting server to use for information related to the link.

Usage: Specify the IP address of an accounting server. The default is 0.0.0.0/0.

Example: `Acct Host=10.2.3.4/24`

Dependencies: The Acct Host setting does not apply unless the Acct Type parameter specifies that a connection-specific server is in use.

Location: Ethernet > Connections > Accounting

See Also: Acct Type

Acct Host #N (N=1–3)

Description: Specifies the IP address of an external accounting server. The DSL Terminator unit first tries to connect to server #1. If it receives no response, it tries to connect to server #2. If it still receives no response, it tries server #3. If the DSL Terminator unit connects to a server other than server #1, it continues to use that server until the server fails to service requests, even if the first server has come online again.

Note: Each address must point to servers of the type specified by the Acct parameter (either TACACS+ or RADIUS).

Usage: Specify an IP address in dotted-decimal notation, separating the optional subnet mask from the address by means of a slash character. The default value is 0.0.0.0, which indicates that no accounting server exists.

Example: `acct host #2 = 10.2.3.4/24`

Dependencies: The Acct Host #N parameter does not apply when Acct=None.

Location: Ethernet > Mod Config > Accounting

See Also: Acct

Acct-ID Base

Description: Specifies whether the numeric base of the RADIUS or call-logging Acct-Session-ID attribute is 10 or 16. The Acct-ID Base setting controls how the Acct-Session-ID attribute is presented to the accounting or call-logging server. For example, a

base-10 session ID is presented as 1234567890, and a base-16 ID as 499602D2. You can set the Acct-ID Base parameter globally and for each connection.

Usage: Specify one of the following values:

- 10 (decimal) specifies that the numeric base is 10. This value is the default.
- 16 (hexadecimal) specifies that the numeric base is 16.

Example: `Acct-ID Base=10`

Dependencies: Consider the following:

- The Acct-ID Base parameter is applies only to RADIUS accounting and call logging. It does not apply to TACACS+.
- Acct-ID Base applies in a Connection profile only if the Acct Type parameter specifies that connection-specific accounting or call-logging information is in use.
- The Acct-Session-ID attribute is defined in the RADIUS accounting specification. See your RADIUS documentation for details.
- Changing the value of the Acct-ID Base parameter while accounting or call-logging sessions are active results in inconsistent reporting between Start and Stop records.

Location: Ethernet > Mod Config > Accounting, Ethernet > Mod Config > Call Logging, Ethernet > Connections > Accounting

See Also: Acct, Acct Type

Acct Key

Description: Specifies a RADIUS or TACACS+ shared secret. A shared secret acts as a password between the DSL Terminator unit and the accounting server.

Usage: Specify the text of the shared secret. The value you specify must match the value assigned in the RADIUS Clients file or the TACACS+ Configuration file.

Example: `Acct Key=Lucent`

Dependencies: The Acct Key parameter applies in a Connection profile only if the Acct Type parameter specifies that connection-specific accounting information is in use.

Location: Ethernet > Mod Config > Accounting, Ethernet > Connections > Accounting

See Also: Acct, Acct Host #N, Acct Type

Acct Max Retry

Description: Specifies the number of times the DSL Terminator unit sends an Accounting Request to the RADIUS server before it gives up. The Acct Max Retry parameter addresses the situation in which the RADIUS accounting server is not responding to the DSL Terminator unit's Accounting Request packets. If the RADIUS accounting backoff queue overflows, the DSL Terminator unit discards Accounting Requests whether or not they have reached the maximum number of retries.

Usage: Specify the maximum number of retries allowed. The default is 0 (zero), which specifies no retry limit.

Example: `Acct max retry = 6`

Dependencies: The Acct Max Retry parameter applies only when the Acct=RADIUS and the other required RADIUS accounting parameters have been configured.

Location: Ethernet > Mod Config > Accounting

See Also: Acct, Acct Checkpoint, Acct Host, Acct Key, Acct Port, Acct Reset Timeout, Acct Src Port, Acct Timeout, Allow Stop Only, Sess Timer

Acct Port

Description: Specifies the UDP port number that the DSL Terminator unit uses in Accounting Requests.

Usage: Specify a UDP port number that matches the port number the accounting daemon uses. For RADIUS, the default value is 1646. For TACACS+, the default value is 49.

Example: `Acct port = 1620`

Dependencies: Acct Port applies in a Connection profile only if the Acct Type parameter specifies that connection-specific accounting information is in use.

Location: Ethernet > Mod Config > Accounting, Ethernet > Connections > Accounting

See Also: Acct, Acct Host #N, Acct Type

Acct Reset Timeout

Description: Specifies how long (in seconds) the DSL Terminator unit uses the secondary RADIUS accounting server (Acct Host #2 or Acct Host #3) before attempting to use the primary RADIUS accounting server (Acct Host #1).

If a timeout occurs while the DSL Terminator unit is waiting for a reply from the primary RADIUS server, the DSL Terminator unit sends an Accounting Request to the RADIUS server defined by Acct Host #2. If the unit receives no reply, it sends the Accounting Request to Acct Host #3. If either of the secondary servers acknowledges the request, the DSL Terminator unit continues to use that server instead of the primary one. At the end of the period specified by Acct Reset Timeout, the DSL Terminator unit sends the next Accounting Request to Acct Host #1.

Usage: Enter the time period in seconds. You can specify a value from 0 to 86400. The default is 0 (zero), which specifies that the DSL Terminator unit does not return to the primary server as long as the secondary server is replying to requests.

Example: `Acct reset timeout = 1000`

Location: Ethernet > Mod Config > Acct

See Also: Acct Host #N

Acct Src Port

Description: Specifies the source port used to send a RADIUS or TACACS+ Accounting Request. You can specify the same source port for Authentication Requests and Accounting Requests.

Usage: Specify a port number from 0 to 65535. The default value is 0 (zero). If you accept the value, the DSL Terminator unit can use any port number from 1024 to 2000.

Example: `Acct src port = 1026`

Location: Ethernet > Mod Config > Accounting

See Also: Auth Src Port

Acct Timeout

Description: Specifies the amount of time the DSL Terminator unit waits for a response to a RADIUS Accounting Request. You can set the Acct Timeout parameter globally and for each connection.

If it does not receive a response within that time, the DSL Terminator unit sends the Accounting Request to the next server's address (for example, server #2). If all RADIUS accounting servers are busy, the DSL Terminator unit stores the Accounting Request and tries again at a later time. It can queue up to 154 requests.

Usage: Specify a number from 1 to 10. The default global value is 0. The default in a Connection profile is 1.

Example: `Acct Timeout=3`

Dependencies: This parameter applies only to RADIUS accounting. Because TACACS+ uses TCP, it has its own timeout method. Also, this parameter applies in a Connection profile only if the Acct Type parameter specifies that connection-specific accounting information will be used.

Location: Ethernet > Mod Config > Accounting, Ethernet > Connections > Accounting

See Also: Acct, Acct Type

Acct Type

Description: Specifies whether to use a connection-specific accounting server for accounting related to this link.

Usage: Specify one of the following values:

- None. Logs information to the accounting server specified in the Ethernet profile. None is the default.
- User. Logs information to the accounting server specified in this Connection profile.
- User+Default. Logs accounting information to both servers.

Example: `Acct Type=User`

Dependencies: Connection-specific accounting options rely on the setup in the Accounting subprofile of the Ethernet profile.

Location: Ethernet > Connections > Accounting

See Also: Nailed-Group, TrnkGrp,

Active

Description: Activates a profile (making it available for use) or a route (adding it to the routing table). A dash appears before each deactivated profile or route.

Usage: Specify Yes or No. No is the default.

- Yes activates the profile or feature, making it available for use.
- No disables the profile or feature, making it unavailable for use.

Example: `Active=Yes`

Location: Ethernet > Connections, Ethernet > Frame Relay, Ethernet > Names / Passwords, Ethernet > Static Rtes

Active Server

Description: Specifies which call-logging server is active.

Usage: Specify Host1, Host2, or Host3. The default is Host1.

- Host1 specifies the call-logging server designated by the Host #1 parameter.
- Host2 specifies the call-logging server designated by the Host #2 parameter.
- Host3 specifies the call-logging server designated by the Host #3 parameter.

Example: `Active Server = Host1`

Dependencies: For Active Server to apply, the Call Log parameter must be set to Yes.

Location: Ethernet > Mod Config > Call Logging

See Also: Call Log

Add Pers

Description: Specifies the number of seconds that average line utilization (ALU) must persist beyond the target utilization threshold before the DSL Terminator adds bandwidth from available channels. When adding bandwidth, the DSL Terminator adds the number of channels specified in the Inc Ch Count parameter.

Usage: Specify a number between 1 and 300. The fa ctory default value is 5 for MP+ calls and 20 for AIM calls with dynamic call management.

Example: Add Pers=10

Dependencies: This parameter is not applicable in a Call profile unless Call Mgm=Dynamic. It is not applicable in a Connection profile unless Encaps=MPP.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options

Location: Call Mgm, Encaps

Adv Dialout Routes

Description: Specifies whether the DSL Terminator unit advertises its IP dialout routes if no trunks are available, or stops advertising (poisons).

Note: This parameter is intended for use when two or more DSL Terminator units on the same network are configured with redundant profiles and routes. It solves a problem that occurred when two or more DSL Terminator units on the same network were configured with redundant profiles and routes. If one of the redundant DSL Terminator units lost its trunks temporarily, it continued to receive outbound packets that should have been forwarded to the redundant DSL Terminator unit.

Usage: Specify one of the following values:

- `Always`: (the default) to always advertise IP routes. Use this setting unless you have redundant DSL Terminator units or do not use dialout routes.
- `Trunks Up`: to stop advertising (*poison*) its IP dialout routes if it temporarily loses the ability to dial out.

Example: `Adv Dialout Routes=Always`

Dependencies: This parameter is not applicable unless the DSL Terminator unit is being used in a redundant configuration.

Location: Ethernet > Mod Config

Aggregate

Description: Specifies how the DSL Terminator determines the bit rate of individual VCs sharing a single traffic shaper.

Usage: Specify one of the following values.

- No (the default) specifies that the bit rate for a VC using this traffic shaper is the value specified in the Bit Rate parameter, provided there is no contention for the bandwidth.
- Yes specifies that each VC using this traffic shaper will be limited to a throughput of Bit Rate/(*number of virtual connections*).

Example: `Aggregatel=No`

Dependencies: The Traffic Shaper profile must be enabled for Aggregate to apply.

Location: Net/DS3-ATM > Line Config > *any line profile* > Traffic Shapers,
Net/OC3-SMF-ATM > Line Config > *any line profile* > Traffic Shapers,
Net/OC3-UTP-ATM > Line Config > *any line profile* > Traffic Shapers

See Also: Bit Rate, Max Burst Size, Peak Rate, Priority, Traffic Shaper

Alarm Threshold

Description: Specifies a number to use as a threshold for generating an SNMP alarm trap as part of the heartbeat monitoring feature. If the number of monitored packets falls below this number, the following SNMP alarm trap is sent:

```
Trap type: TRAP_ENTERPRISE
Code: TRAP_MULTICAST_TREE_BROKEN (19)
Arguments:
1) Multicast group address being monitored (4 bytes),
2) Source address of last heartbeat packet received (4 bytes)
3) Slot time interval configured in seconds (4 bytes),
4) Number of slots configured (4 bytes).
5) Total number of heartbeat packets received before the unit
started sending SNMP Alarms (4bytes).
```

When it is running as a multicast forwarder, the DSL Terminator unit is continually receiving multicast traffic. The heartbeat-monitoring feature enables the administrator to monitor possible connectivity problems by polling continuously for this traffic and generating an SNMP alarm trap if there is a traffic breakdown.

Note: Heartbeat monitoring is optional. It is not required for multicast forwarding.

Usage: Specify a number.

Example: `Alarm Threshold=3`

Dependencies: To set up heartbeat monitoring, you must configure several parameters that define what packets will be monitored, how often and for how long to poll for multicast packets, and the threshold for generating an alarm. These parameters do not apply if multicast forwarding is not in use.

Location: Ethernet > Mod Config > Multicast

See Also: HeartBeat Addr, HeartBeat Udp Port, HeartBeat Slot Time, HeartBeat Slot Count, Source Addr, Source Mask

All Port Diag

Description: Enables or disables a permission that allows an operator to perform all port diagnostic commands listed in the Port Diag menu.

Usage: Specify Yes or No. Yes is the default.

- Yes means the operator can perform all diagnostic commands in the Port Diag menu.
- No means the operator cannot use those commands.

Example: `All Port Diag=Yes`

Dependencies: This parameter is not applicable if the Operations permission is disabled.

Location: System > Security

See Also: Own Port Diag

Allow as Client DNS

Description: Specifies whether the local DNS servers should be made accessible to PPP connections if the client DNS servers are unavailable.

Client DNS parameters configure DNS server addresses that will be presented to WAN connections during IPCP negotiation. They provide a way to protect your local DNS information from WAN users. Client DNS has two levels: a global configuration that applies to all PPP connections, and a connection-specific configuration that applies to that connection only. The global client addresses are used only if none are specified in the Connection profile.

The allow as Client DNS parameter acts as a flag to enable the DSL Terminator unit to present the local DNS servers to the WAN connection when all client DNS servers are undefined or unavailable.

Usage: Specify Yes or No. No is the default.

- Yes allows clients to use the local DNS servers.
- No prevent clients from using the local DNS servers.

Example: `Allow as Client DNS=No`

Location: Ethernet > Mod Config > DNS

See Also: Client Assign DNS, Client Pri DNS, Client Sec DNS

Allow Stop Only

Description: Specifies whether the DSL Terminator unit can send accounting or call-logging Stop packets without a username to the RADIUS or call-logging server. Typically, the DSL Terminator unit sends both a Start and a Stop packet to the RADIUS accounting or call-logging server to record a connection. User authentication is required before a Start packet is sent, so when the connection is terminated before authentication occurs or when the name and password supplied by the user is rejected, the Start packet is not sent and the Stop packet contains no username.

Usage: Specify one of the following values:

- Yes allows the DSL Terminator unit to send Stop Accounting Packets that do not contain a username.
- No allows the DSL Terminator unit to send any type of Account Request Packet the DSL Terminator unit can send. This is the default.

Example: `Allow Stop Only=Yes`

Location: Ethernet > Mod Config > Accounting, Ethernet > Mod Config > Call Logging

See Also: Acct, Acct Checkpoint, Acct Host, Acct Key, Acct Port, Acct Reset Timeout, Acct Src Port, Acct Timeout, Sess Timer

AnsOrig

Description: Specifies whether the DSL Terminator unit enables incoming calls, outgoing calls, or both for this connection.

Usage: Specify one of the following values:

- Both specifies that the DSL Terminator unit can initiate calls to the destination specified in the Connection profile, and that the DSL Terminator unit can receive calls from that destination as well.

  Both is the default.
- Call Only specifies that the DSL Terminator unit can dial out to the destination specified in the Connection profile, but cannot answer calls from that destination.

Ans Only specifies that the DSL Terminator unit can receive calls from the destination specified in the Connection profile, but cannot initiate calls to that destination.

Example: `AnsOrig=Both`

Dependencies: This parameter is not applicable for leased connections.

Location: Ethernet > Connections > Telco Options

See Also: LAN Adrs, Station

Apply To

Description: Specifies the direction in which Type-of-Service (TOS) is enabled.

Usage: Specify one of the following values:

- Input (the default) specifies that bits are set in packets received on the interface.
- Output specifies that bits are set in outgoing packets only.
- Both specifies that both incoming and outgoing packets are tagged.

`Example:` `Apply To=Input`

Location: Ethernet > Connections > IP Options

Ascend

Description: Specifies whether a trap is generated to indicate a change of state in a host interface. All port connections are monitored in a state machine and reported via this trap.

Usage: Specify Yes or No. The default is Yes.

- Yes specifies that a trap is generated to indicate a change of state in a host interface.
- No specifies that a trap is not generated to indicate a change of state in a host interface.

Example: `Ascend=Yes`

Location: Ethernet > SNMP Traps > Enable Traps

See Also: Console

Ascend-PPPoE-Enable (74)

Description: Specifies whether the unit responds to PPPoE packets associated with the user profile. The Ascend-PPPoE-Enable attribute appears in an Access-Accept packet.

Usage: Specify one of the following values:

- PPPoE-Yes (1) specifies that the unit responds to PPPoE packets associated with the user profile.
- PPPoE-No (0) specifies that the unit does not respond to PPPoE packets associated with the user profile.

Example: `Ascend-PPPoE-Enable (74)=Yes`

Dependencies: Ascend-PPPoE-Enable is not applicable if bridging is turned off for the interface.

Ascend-Bridge-Non-PPPoE (75)

Description: Specifies whether the DSL Terminator bridges packets other than PPPoE for the user profile. The Ascend-Bridge-Non-PPPoE attribute appears in an Access-Accept packet.

Usage: Specify one of the following settings:

- Bridge-Non-PPPoE-Yes (1) specifies that the DSL Terminator bridges packets other than PPPoE for the user profile.
- Bridge-Non-PPPoE-No (0) specifies that the DSL Terminator does not bridge packets other than PPPoE for the user profile.

Example: `Ascend-Bridge-Non-PPPoE (75)=Yes`

Dependencies: Ascend-Bridge-Non-PPPoE does not apply if bridging is turned off on the interface, or if Ascend-PPPoE-Enable=PPPoE-No (0).

Assign Adrs

Description: Enables or disables dynamic IP address assignment for incoming calls.

Usage: Specify Yes or No. No is the default.

- Yes enables the DSL Terminator unit to assign an IP address to an incoming PPP call that requests dynamic assignment, provided it has access to a pool of designated IP address.
- No disables dynamic IP address assignment.

Example: `Assign Adrs=Yes`

Dependencies: The DSL Terminator unit must have at least one configured pool of IP addresses, either locally or on a RADIUS server.

Location: Ethernet > Answer

See Also: Encaps, LAN Adrs, Pool # Count(N=1-10), Pool #N Start(N=1-10), Recv Auth, WAN Alias

AT Answer String

Description: Enables you to add customized AT commands in the answer string of the system's modem configuration:

Usage: Specify one or more valid AT commands, up to a limit of 36 characters. The default is null.

Example: `AT Answer String`

Dependencies: Consider the following:

- Do not begin the string with the characters *AT*. These two characters are automatically added to the beginning of the string, before the DSL Terminator sends the commands to the modem.
- Do not include an A (answer) or a D (dial) command anywhere in the string. An A command is automatically added to the end of the string. A D command in the answer string causes the call to fail.
- The answer string is the last of four strings sent to the modem when the DSL Terminator answers a call. Therefore, the commands you enter can overwrite settings specified elsewhere.
- Be very careful when entering AT commands for AT Answer String. The system does not prevent you from entering incorrect strings.

Location: System > Sys Config

ATMP Gateway

Description: Instructs the DSL Terminator unit to send data it receives back from the home network on this connection to the mobile node.

Usage: Specify Yes or No. No is the default.

- Yes enables the DSL Terminator unit to send data it receives back from the home network on this connection to the mobile node.
- No disables this function.

Example: `ATMP Gateway=Yes`

Dependencies: This parameter is not applicable unless the DSL Terminator unit is configured as an ATMP Home Agent in gateway mode.

Location: Ethernet > Connections > Session Options

See Also: ATMP Mode, Password, Type, UDP Port

ATMP Mode

Description: Specifies whether Ascend Tunnel Management Protocol (ATMP) is enabled and, if so, whether this unit is a Home Agent, a foreign agent, or both.

Usage: Specify one of the following values:

- Disabled (the default) specifies that ATMP is not enabled.
- Home specifies that this unit is a Home Agent.
- Foreign specifies that this unit is a foreign agent.
- Both specifies that the DSL Terminator unit will function as both a Home Agent and foreign agent on a tunnel-by-tunnel basis.

Example: `ATMP Mode=Home`

Dependencies: If you set ATMP Mode=Disabled, all other fields in the ATMP Options menu are not applicable.

Location: Ethernet > Mod Config > ATMP Options

See Also: ATMP Gateway, Password, Type, UDP Port

ATMP RIP

Description: Specifies whether to use RIP-2 for the Home Agent's Gateway-Profile in an Ascend Tunnel Management Protocol (ATMP) configuration.

Usage: Specify one of the following values:

- Off (the default) specifies that the profile does not use RIP.
- Send-v2 specifies that the Home Agent constructs a RIP-2 Response(2) packet at every RIP interval and sends it to the Home Network from all tunnels using the Gateway-Profile. For each tunnel, the Response packet contains the Mobile-Client IP address, the subnet mask, the next hop set to 0.0.0.0, and the metric set to 1. There is no support for RIP-2 authentication or route tag.

Example: `ATMP Rip=Off`

Dependencies: The Home Network router should not send RIP updates, because the Home Agent does not inspect them. The RIP updates would be forwarded to the Mobile Clients instead.

Location: Ethernet > Connections > Session Options

See Also: ATMP Gateway, ATMP Mode

ATMP SNMP Traps

Description: Specifies that the DSL Terminator sends ATMP-related SNMP traps.When a user attempts to telnet into the MAX for management purposes and fails, the MAX generates an SNMP trap. The SNMP trap indicates that a user has failed to access the box, but does not give an indication as to who accessed it. By including the IP address of the originating station, it indicates where the session originated. This is not a direct translation to "who", but it provides some general information.

The following SNMP message will be sent to all SNMP Trap clients that are enabled for Security messages.

```
mmm.mmm.mmm.mmm  Enterprise Specific Trap (15) Uptime: xx:xx:xx
Name .iso.org.dod.internet.private.enterprises.ascend.
   sessionStatusGroup.sessionStatusTable.
   sessionStatusEntry.ssnStatusUserIPAddress%d
IpAddress: ttt.ttt.ttt.ttt
```

where mmm.mmm.mmm.mmm = Host's IP address

ttt.ttt.ttt.ttt = Telnet client's IP address

%d = attemped Telnet session number

Usage: Specify Yes or No.

- Yes means that the DSL Terminator sends ATMP-related SNMP traps.
- No means that the DSL Terminator does not send ATMP-related SNMP traps.

Example: `ATMP SNMP Traps = No`

Location: Ethernet > Mod Config > ATMP options

Auth

Description: Specifies the type of external authentication server to access for incoming connections.

Usage: Specify one of the following values:

- `None`— (the default) disables the use of an authentication server.
- `TACACS`— Accesses a TACACS server. TACACS supports PAP, but not CHAP authentication.
- `TACACS+`— Accesses a TACACS+ server. TACACS+ supports PAP, but not CHAP authentication and provides more extensive accounting statistics and a higher degree of control than TACACS authentication.
- `RADIUS` — Accesses a RADIUS server. In a RADIUS query, the DSL Terminator unit provides a user ID and password to the server. If the validation succeeds, the server sends back a complete profile; this profile specifies routing, packet filtering, destination-specific static routes, and usage restrictions for the user. RADIUS supports PAP and CHAP.
- `RADIUS/LOGOUT`— accesses a RADIUS server. This setting is identical to RADIUS, except that when you select Radius-Logout, the DSL Terminator unit sends a request to the RADIUS server to initiate logout when the session ends.

  Use this setting to set up an AppleTalk Remote Access connection to a SecurID server using RADIUS.
- `Defender`— Accesses a Digital Pathways Defender authentication server.
- `SECURID`— Accesses a SecurID ACE server.

Example: `Auth=RADIUS` (for authentication using RADIUS), `Auth=RADIUS/LOGOUT` (for authentication using RADIUS and a SecurID server).

Dependencies: This parameter requires a server address in an Auth Host # parameter.

Location: Ethernet > Mod Config > Auth

See Also: Auth Host, Auth Key, Auth Port, Auth Timeout, Encaps

Auth Compat Mode

Description: Enables or disables Vendor-Specific Attribute (VSA) compatibility mode when the DSL Terminator unit is using RADIUS for authentication and authorization purposes.

Usage: Specify one of the following settings:

- `Old`—(the default) specifies that the DSL Terminator unit does not send the Vendor-Specific attribute to the RADIUS server and does not recognize the Vendor-Specific attribute if the server sends it.
- `Vendor-Specific`—specifies that the DSL Terminator unit uses the Vendor-Specific Attribute to encapsulate Lucent vendor attributes, and uses the RFC-defined User-Password encryption algorithm as well.

Example: `Auth Compat Mode=Old`

Location: Ethernet > Mod Config > Auth

See Also: Acct Compat Mode, Compat Mode

Auth Host #N (N=1–3)

Description: Each of these parameters specifies the IP address of an external authentication server. The DSL Terminator unit first tries to connect to server #1. If it receives no response, it tries to connect to server #2. If it receives no response, it tries server #3. If the DSL Terminator unit connects to a server other than the server #1, it continues to use that server until it fails to service requests, even if the first server has come online again.

Note: The addresses must all point to servers of the same type, as specified in the Auth parameter (RADIUS, TACACS, or TACACS+). If you are using Defender or SecurID authentication, only Auth Host #1 is applicable, because the DSL Terminator unit can access only one of those servers.

Usage: Specify an IP address in dotted-decimal format, separating the optional netmask with a slash character. The default value is 0.0.0.0; this setting indicates that no authentication server exists.

Example: `Auth Host #1=10.207.23.6`

Dependencies: This parameter does not apply if authentication services are disabled.

Location: Ethernet > Mod Config > Auth

See Also: Auth, Auth Port, Auth Timeout

Auth Key

Description: Specifies an authentication key, which is typically a shared secret with the authentication server.

- For RADIUS, this is a string up to 22 characters. Because the DSL Terminator unit can act both as a client to external servers and as an on-board server responding to client commands, this parameter is configured in two places for RADIUS.
- If the DSL Terminator unit is acting as a TACACS or TACACS+ client, this is a password supplied by the DSL Terminator unit to the server.
- If the DSL Terminator unit is acting as a Defender client, this is a DES secret key shared between the DSL Terminator unit and the Defender authentication server. This key is also used for authentication by the DSL Terminator unit in its role as a Defender authentication agent.
- If the DSL Terminator unit is acting as a SecurID client, this parameter is not applicable. See SecurID DES Encryption and SecurID Node Secret for details.

Usage: Specify the authentication key.

Example: `Auth Key=Lucent`

Dependencies: This value of this parameter depends on the setting of the Auth parameter. If Auth is set to SECURID, this parameter is not applicable.

Location: Ethernet > Mod Config > Auth

See Also: Auth, Auth Host, Auth Port, Auth Timeout, SecurID DES Encryption, SecurID Node Secret

Auth Pool

Description: Enables or disables dynamic address assignment for RADIUS-authenticated IP routing connections. The RADIUS server must be configured with at least one pool of addresses for assignment, and must be running the Lucent daemon.

Usage: Specify Yes or No. No is the default.

- Yes means a dial-in host can obtain an IP address dynamically from the RADIUS server.
- No disables dynamic IP address assignment for RADIUS-authenticated connections.

Example: `Auth Pool=Yes`

Location: Ethernet > Mod Config > Auth

See Also: Auth

Auth Port

Description: Specifies the UDP or TCP port to use to communicate with the external authentication server. It must match the port specified for use in the server's configuration.

- If the DSL Terminator unit is acting as a RADIUS client, this is the UDP destination port to use for authentication. The UDP port used by RADIUS daemons is specified in the /etc/services file (UNIX).

- If the DSL Terminator unit is acting as a TACACS or TACACS+ client, it specifies the UDP destination port to use for authentication (49 by default).
- If the DSL Terminator unit is acting as a RADIUS server, this is the UDP port to use for the on-board RADIUS server. (The on-board server is a mechanism that allows the DSL Terminator unit to respond to messages from the *radius* daemon. It is set to 1700 by default.
- If the DSL Terminator unit is acting as a Defender client, this is the TCP port to use to communicate with the server. It is set to 2626 by default.
- If the DSL Terminator unit is acting as a SecurID client, this is the TCP port to use to communicate with the server. It is set to 5500 by default.

Note: Make sure that the number you specify matches what is actually in use by the authentication server daemon.

Usage: Specify the port number used by the server.

Example: `Auth Port=1565`

Location: Ethernet > Mod Config > Auth

See Also: Auth, Auth Host, Auth Timeout

Auth Reset Timeout

Description: Specifies the authentication-timeout period in seconds, after which the DSL Terminator unit returns to the primary RADIUS authentication server.

Usage: Specify the number of seconds. The default is 0 (zero), which specifies that the DSL Terminator unit does not return to using the primary RADIUS authentication server.

Example: `Auth Reset Timeout=500`

Dependencies: For Auth Reset Timeout to apply, you must specify at least one value for Auth Host.

Location: Ethernet > Mod Config > Auth

Auth Send Attr 6,7

Description: Specifies whether the DSL Terminator unit sends values for RADIUS attributes 6 and 7. Typically, it generates appropriate values for RADIUS attribute 6 (user-service) and 7 (framed-protocol) and includes them in Authentication Requests for incoming calls. To support RADIUS servers that should not receive that information, you can disable this behavior.

Usage: Specify Yes or No. Yes is the default.

- Yes causes attributes 6 and 7 to be sent to the RADIUS Server in the Authentication Request. Use this setting if you use a MERIT RADIUS server.
- No excludes attributes 6 and 7 from Authentication Requests.

Example: `Auth Send Attr 6,7=Yes`

Dependencies: This parameter applies only to RADIUS authentication.

Location: Ethernet > Mod Config > Auth

Auth Src Port

Description: Specifies the source port used to send a remote Authentication Requests. You can define a source port for all the external authentication services the DSL Terminator unit supports. You can specify the same source port for authentication and Accounting Requests.

Usage: Specify a port number between 0 and 65535. The default value is 0 (zero); if you accept this value, the DSL Terminator unit can use any port number between 1024 and 2000.

Example: `Auth Src Port=0`

Dependencies: This parameter does not apply if external authentication is not in use.

Location: Ethernet > Mod Config > Auth

See Also: Acct Src Port

Auth Timeout

Description: Specifies the number of seconds between retries to the external authentication server.

- If the DSL Terminator unit is acting as a RADIUS, TACACS, or TACACS+ client, the DSL Terminator unit waits the specified number of seconds for a response to an Authentication Request. If it does not receive a response within that time, it times out and sends the Authentication Request to the next authentication server (for example, Auth Host #2).
- If the DSL Terminator unit is acting as a Defender or SecurID client (each type supports only one server address), the DSL Terminator unit waits the specified number of seconds before assuming that the server has become nonfunctional. For more information about SecurID timeouts, see SecurID Host Retries parameter.

Note: Because remote authentication is tried first if the Local Profiles First parameter is set to No, the DSL Terminator unit waits for the remote authentication to time out before attempting to authenticate locally. This timeout might take longer than the timeout specified for the connection and might cause all connection attempts to fail. To prevent this, set the authentication timeout value low enough not to cause the line to be dropped, but still high enough to permit the unit to respond if it is able. The recommended time is 3 seconds.

Usage: Specify a number from 1 to 10. The default is 1.

Example: Auth Timeout=20

Dependencies: This parameter applies only when using an external authentication server.

Location: Ethernet > Mod Config > Auth

See Also: Auth, Auth Host , Auth Port, SecurID Host Retires.

Auto Logout

Description: Specifies whether the DSL Terminator unit automatically logs a user out when a device disconnects from the DSL Terminator unit's control port or when the unit loses power.

Usage: Specify Yes or No. No is the default.

- Yes enables the DSL Terminator unit to log out the current user and go back to default privileges when a device disconnects from the unit's control port or when the unit loses power.
- No disables auto-logout.

Example: `Auto Logout=Yes`

Location: System > Sys Config

Aux Send PW

Description: Specifies the password the DSL Terminator unit sends when it adds channels to a multichannel PPP call that uses PAP-TOKEN-CHAP authentication. The unit obtains authentication of the first channel of this call from the user's hand-held security card.

Usage: Specify a password. This password must match the one set up for your DSL Terminator unit in the RADIUS users file on the NAS (network authentication server).

Example: `Aux Send PW=Lucent`

Dependencies: This parameter applies only to multichannel PPP calls.

Location: Ethernet > Connections > Encaps Options

See Also: Send Auth

B

Backup

Description: Specifies the number of a backup Connection profile for a nailed connection. It is intended as a backup if the far end device goes out of service, in which case the backup call is made. It is not intended to provide alternative lines for getting to a single destination.

Note: A Connection profile's number is the unique portion of the number preceding the profile's name in the Connections menu.

Usage: Specify the Connection profile number. The default value is null.

Example: `Backup=22`

Location: Ethernet > Connections > Session Options

See Also: Name

BACP

Description: Enables or disables the Bandwidth Allocation Control Protocol (BACP).

Usage: Specify Yes to enable BACP. No is the default.

Example: `BACP=Yes`

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options

Base Ch Count

Description: Specifies the number of channels to use to set up a session initially.

Usage: Specify a number from 1 to 32. The default is 1.

Example: `Base Ch Count=2`

Dependencies: This parameter does not apply for leased connections.

Location: Ethernet > Connections > Encaps Options

See Also: Max Ch Count

Bi-Dir Auth

Description: Specifies whether CHAP authentication must be bidirectional.

Usage: Specify one of the following values:

- None (the default) specifies that authentication is unidirectional. The called device identifies the calling one. The DSL Terminator unit prevents the authentication in which the calling party identifies the called party.
- Allowed specifies that authentication can be bidirectional.

When the DSL Terminator unit is the called device, the DSL Terminator unit identifies the calling device. The system also allows the calling device to authenticate the DSL Terminator unit, but this authentication is not mandatory. Therefore, if the calling device does not authenticate the DSL Terminator unit, the DSL Terminator unit can still accept the call.

When the DSL Terminator unit is the calling device, the DSL Terminator unit answers the authentication initiated by the called device. The DSL Terminator unit tries to negotiate authentication in the opposite direction as well, but if the called device refuses this second authentication option, the call is still established.

- Required specifies that authentication must be bidirectional. The DSL Terminator unit requires that both the calling and called devices authenticate each other. If authentication is not performed in both directions, the DSL Terminator unit rejects the call (in the case of an incoming call) or tears down the call (in the case of an outgoing call).

Example: `Bi-Dir Auth=None`

Dependencies: Consider the following:

- If you specify Allowed or Required, and the second authentication is attempted, it must be successful. Otherwise, the DSL Terminator unit rejects the call (in the case of an incoming call) or tears down the call (in the case of an outgoing call).
- Bidirectional authentication is applicable only if the authentication mode is CHAP, MS-CHAP, or CACHE-TOKEN.
- When Receive Auth is set to Either, and PAP authentication is negotiated, bidirectional authentication is automatically disabled, even if the Bi-Dir Auth is set to Required. For example, suppose you set Receive Auth to Either, and Bi-Dir Auth to Required. If an incoming call occurs and the authentication negotiated is PAP, the authentication will be done in one direction only.
- Bi-Dir Auth is not applicable if PPP is not enabled, or if Receive Auth is set to None, PAP, PAP-Token, or PAP-Token-CHAP.

Location: Encaps > Answer > PPP-Options, Ethernet > Connection > PPP Options

See Also: Receive Auth, Recv Name

Bill

Description: Specifies a telephone number to be used for billing purposes. If a number is specified, it is used either as a billing suffix or the calling party number. For robbed-bit lines, the DSL Terminator uses the billing-number as a suffix that is appended to each phone number it dials for the call.

For PRI lines, the DSL Terminator uses the billing-number parameter rather than the phone number ID to identify itself to the answering party.

If the calling party uses the billing-number parameter instead of its phone number as its ID, the CLID used by the answering side is not the true phone number of the caller. This situation presents a security breach if you use CLID authentication. Further, be aware that if you specify a value for the billing-number parameter, there is no guarantee that the phone company will send it to the answering device.

Note: For outgoing calls on a PRI line, the value of the Bill # parameter in the Dial Plan profile overrides the value of the Bill # parameter in the Call profile and Connection profile.

Usage: Specify the billing number provided by the carrier. You can enter up to 24 characters. The default value is null.

Example: `Bill #=666`

Location: Ethernet > Connections > Telco Options, System > Dial Plan, Ethernet > Frame Relay, Ethernet > X.25

See Also: Calling #, Clid Auth

Bit Rate

Description: Specifies the average bit rate (in kbps) at which the virtual circuit using a Traffic Shaping profile transmits data.

Usage: Specify a value (in kbps) from 0 (zero) to the maximum rate the interface supports. For a DS3-ATM card the maximum is 37290; for the OC3-ATM card the maximum rate is 135631. The default is 1000.

Example: `Bit Rate=2000`

Dependencies: The Traffic Shaper profile must be enabled for Bit Rate to apply.

Location: Net/DS3-ATM > Line Config > *any line profile* > Traffic Shapers, Net/OC3-SMF-ATM > Line Config > *any line profile* > Traffic Shapers, Net/OC3-UTP-ATM > Line Config > *any line profile* > Traffic Shapers

See Also: Aggregate, Enabled, Max Burst Size, Peak Rate, Priority, Traffic Shapers

Block Calls After

Description: Specifies how many unsuccessful attempts the DSL Terminator unit will make before beginning to block outgoing calls.

Usage: Enter the number of connection attempts permitted before the DSL Terminator unit blocks calls for the connection. The maximum number you can enter is 65535 (65535 attempts). The default is 0.

Example: `Block Calls After =100`

Location: Ethernet > Connections > Session Options

Blocked Duration

Description: Specifies the length of time in seconds during which the DSL Terminator unit will block outgoing calls.

Usage: Enter the number of seconds for the DSL Terminator unit to block all calls made to the connection. When this period has elapsed, the unit will again allows calls to this connection.

Example: `Blocked Duration=100`

Location: Ethernet > Connections > Session Options

See Also: Block calls after

BOOTP Relay Enable

Description: Specifies whether Bootstrap Protocol (BOOTP) requests are relayed to other networks. If you enable BOOTP relay, you must also specify the address of at least one BOOTP server in the Server parameter.

Usage: Specify Yes or No. No is the default.

- Yes enables the DSL Terminator unit to relay BOOTP requests to a server on another network.
- No disables BOOTP relay.

Example: `BOOTP Relay Enable=Yes`

Dependencies: For the BOOTP relay feature to work, SLIP BOOTP must be disabled.

Location: Ethernet > Mod Config > BOOTP Relay

See Also: Server

Bridge

Description: Enables or disables link-level packet bridging for this connection. If you disable bridging, you must enable routing. Enabling bridging in the Answer profile enables the DSL Terminator unit to answer a call that contains packets other than IP.

Usage: Specify Yes or No. No is the default.

- Yes enables the DSL Terminator unit to bridge packets across this connection based on the packet's destination MAC address (if specified in a Connection profile) or to answer incoming bridged connections (if specified in the Answer profile).
- No disables link-level bridging.

Example: `Bridge=Yes`

Dependencies: This parameter does not apply unless the Bridging parameter is enabled in the Ethernet profile.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections

See Also: Bridging, Encaps, Route IP

Bridge Group

Description: Specifies the bridge group assigned to the Ethernet interface (Mod Config profile) or the connection (Connection profile). Bridge groups give you the ability to group several bridged connections or Ethernet ports into one logical bridge.

Usage: Specify a number from 0 to 2000.

Example: `Bridge Group=12`

Dependencies: Keep this additional information in mind.

- Bridge Groups does not apply if Bridging is set to No in the Ethernet > Mod Config profile.
- Bridge Groups in a Connection profile does not apply if Bridge is set to No in the Connection profile.

Location: Ethernet > Mod Config > Ether1 options, Ethernet > Mod Config > Ether2 options, Ethernet > Connections > *any Connection profile* > Bridge Options

See Also: Enabled, Proxy ARP

Bridging

Description: Enables or disables systemwide packet-bridging . It causes the DSL Terminator unit's Ethernet controller to run in promiscuous mode. In promiscuous mode, the Ethernet driver accepts all packets regardless of address or packet type and passes them up the protocol stack for a higher-layer decision on whether to route, bridge, or reject the packets.

Note: Running in promiscuous mode incurs greater processor and memory overhead than the standard mode of operation for the Ethernet controller. On heavily loaded networks, this increased overhead can result in slower performance, even if no packets are actually bridged.

Usage: Specify Yes or No. No is the default.

- Yes enables the DSL Terminator unit to bridge packets based on MAC addresses by running its Ethernet controller in promiscuous mode, which causes it to accept all packets regardless of packet type or address.
- No disables packet bridging and turns off promiscuous mode in the Ethernet controller.

Example: `Bridging=Yes`

Location: Ethernet > Mod Config

See Also: Bridge

Buildout

Description: Specifies the line buildout value for T1 lines with an internal CSU (Channel Service Unit). The buildout value is the amount of attenuation the DSL Terminator unit should apply to the line's network interface in order to match the cable length from the unit to the next repeater.

Attenuation is a measure of the power lost on a transmission line or on a portion of that line. When you specify a build-out value, the DSL Terminator unit applies an attenuator to the T1 line, causing the line to lose power when the received signal is too strong. Repeaters boost the signal on a T1 line. If the DSL Terminator unit is too close to a repeater, you need to add some attenuation.

Usage: Check with your carrier to determine the correct value for this parameter. Specify one of the following decibel values:

- 0 (the default)
- 7.5
- 15

- 22.5

Example: `Buildout=0`

Dependencies: This parameter is applicable only if the T1 line has an internal CSU to connect to the local digital telephone system, and Front End=CSU.

Location: Net/8T1 > Line Config > Line *N*

See Also: Clock Source, Encoding, Framing Mode, Front End, Length

Bundle Name

Description: Specifies the name of a multilink Frame Relay bundle, up to 15 characters, which must be unique systemwide.

In a Multi-Link FR profile, the Bundle Name parameter defines a name for the bundle. In the Frame Relay profile, the name makes the datalink a member of the MFR bundle. (All member datalinks specify the same bundle name.)

Usage: Specify the name of a Multi-Link FR profile (up to 15 characters).

Example: `Bundle Name=`**`sdsl-mfr`**

Dependencies: All member datalinks must specify the name of the same Multi-Link FR profile. In a Multi-Link FR profile, the name must be unique systemwide.

Location: Frame-Relay, Multi-Link FR

See Also: Active, MFR Type, Max Members, Min Bandwdth

C

Call-by-Call

Description: In a T1 Line profile, specifies the call-by-call signaling value to set for routing calls from a local device through the DSL Terminator to the network. When it is set in another profile, it specifies the PRI service to use when placing a call using that profile.

Note: The Call-by-Call setting in the Dial Plan profile overrides the Call-by-Call setting in the Call and Connection profiles.

These are the call-by-call services available if the service provider is AT&T:

- 0 (Disable call-by-call service)
- 1 (SDN, including GSDN)
- 2 (Megacom 800)
- 3 (Megacom)
- 6 (ACCUNET Switched Digital Services)
- 7 (Long Distance Service, including AT&T World Connect)
- 8 (International 800—I800)
- 16 (AT&T MultiQuest)

These are the VPN and GVPN call-by-call services available if the service provider is Sprint:

- 0 (Reserved)
- 1 (Private)
- 2 (Inwatts)
- 3 (Outwatts)
- 4 (FX)
- 5 (Tie Trunk)

These are the call-by-call services available if the service provider is MCI:

- 1 (VNET/Vision)
- 2 (800)
- 3 (PRISM1, PRISM II, WATS)
- 4 (900)
- 5 (DAL)

Usage: Specify a number between 0 and 65535, corresponding to the type of call-by-call service in use. The factory default is 0, which disables call-by-call service.

Example: `Call-by-Call=6`

Location: Ethernet > Connections > Telco Options, System > Dial Plan, Ethernet > Frame Relay, Net/T1 > Line Config > Line *N*, Ethernet > X.25

See Also: Call-by-Call *N*

Call-by-Call N (N=1–6)

Description: In a Destination profile, specifies the PRI service to use when placing a call using the associated Dial #. For example, when the DSL Terminator dials the number specified by Dial 5#, the DSL Terminator uses the services specified by Call-by-Call 5.

Note: The setting of the Call-by-Call *N* parameter in the Destination profile overrides the setting of the Call-by-Call parameter in the Call profile or Connection profile.

These are the call-by-call services available if the service provider is AT&T:

- 0 (Disable call-by-call service)
- 1 (SDN, including GSDN)
- 2 (Megacom 800)
- 3 (Megacom)
- 6 (ACCUNET Switched Digital Services)
- 7 (Long Distance Service, including AT&T World Connect)
- 8 (International 800—I800)
- 16 (AT&T MultiQuest)

These are the VPN and GVPN call-by-call services available if the service provider is Sprint:

- 0 (Reserved)
- 1 (Private)
- 2 (Inwatts)
- 3 (Outwatts)
- 4 (FX)
- 5 (Tie Trunk)

These are the call-by-call services available if the service provider is MCI:

- 1 (VNET/Vision)
- 2 (800)
- 3 (PRISM1, PRISM II, WATS)
- 4 (900)
- 5 (DAL)

Usage: Specify a number between 0 and 65535, corresponding to the type of call-by-call service in use. The factory default is 0, which disables call-by-call service.

Example: `Call-By-Call 1=4`

Location: System > Destinations

See Also: Call-by-Call, Option

Call Filter

Description: Specifies the number of a filter used to determine if a packet should reset the idle timer or a call. If both a call filter and data filter are applied to a connection, the DSL

Terminator unit applies a call filter after applying a data filter. (Only those packets that the data filter forwards can reach the call filter.)

Usage: Specify a number between 0 and 199. The number you enter depends on the whether you are applying a filter you created using the VT100 interface or a firewall you created using Secure Access Manager (SAM).

If you are applying a filter created using the VT100 interface, enter the last two digits of the filter number as it appears in the Filters menu.

If you are applying a firewall created with SAM, add 100 to the last two digits of the firewall number as it appears in the Firewalls menu. For example, if the number of your firewall is 90-601, specify 101. Refer to your SAM documentation for information on downloading firewalls to the DSL Terminator unit. The numbering scheme for filters and firewalls is:

- 0 indicates that no filtering is being used (this is the default)
- 1-99 indicates that a filter created using the VT100 interface is being used
- 100-199 indicates that a filter created using SAM is being used.

Example: `Call Filter=7`

Location: Ethernet > Answer > Session Options, Ethernet > Connections > Session Options

See Also: Data Filter, Filter

Call Log

Description: Enables or disables call logging.

Usage: Specify Yes or No. No is the default.

- Yes enables call logging.
- No disables call logging.

Example: `Call Log=Yes`

Dependencies: If you set Call Log=Yes, you must specify the IP address of at least one call-log host for the Host # *N* setting.

Location: Ethernet > Mod Config > Call Logging

See Also: Acct-ID Base, Allow Stop Only, Call Log Timeout, Dst Port, Host # N, Key, Max Retry, Reset Timeout

Call Log Timeout

Description: Specifies the amount of time (in seconds) that the DSL Terminator unit waits for a response to a call-logging request.

If it does not receive a response within the specified time, the DSL Terminator unit sends the request to the next host specified by the Host #*N* parameter. If all call-logging hosts are busy, the DSL Terminator unit stores the request and tries again at a later time. It can queue up to 154 requests.

Usage: Specify an integer from 1 to 10. The default, 0 (zero), disables the timer.

Example: `Call Log Timeout`

Dependencies: If Call Log=No, Call Log Timeout does not apply.

Location: Ethernet > Mod Config > Call Logging

See Also: Acct-ID Base, Allow Stop Only, Call Log, Dst Port, Host # N, Key, Max Retry, Reset Timeout

Call Type

Description: Specifies a type of connection.

Usage: Specify Nailed, Switched, Nailed/MPP, or Perm/Switched:

- `Nailed`—The default for Frame Relay profiles, consisting of nailed-up channels. You must specify which nailed channels to use in the Group or Nailed Grp parameter.
- `Switched`—The default in a Connection profile (a link that consists of switched channels).
- `Nailed/MPP`—nailed channels that may be augmented with switched channels if bandwidth is needed during an MP+ call. A Nailed/MPP connection is established when its nailed *or* switched channels are connected end-to-end. The switched channels are dialed when the DSL Terminator unit receives an outbound packet for the far end and cannot forward it across the nailed connection, either because those channels are down or because they are being fully utilized.

  If both the nailed and switched channels in a Nailed/MPP connection are down, the connection does not reestablish itself until the nailed channels are brought back up or the switched channels are dialed. The maximum number of channels for the Nailed/MPP connection is either the value of the Max Ch Count parameter or the number of nailed channels in the specified group, whichever is greater. If a nailed channel fails, the DSL Terminator unit replaces that channel with a switched channel, even if the call is online with more than the minimum number of channels.

  The DSL Terminator unit must be the originator of the switched call. If you modify a Nailed/MPP Connection profile, most changes become active only after the call is brought down and then brought back up.
- `Perm/Switched` —(This parameter is found in the Connection profile only). A permanent switched connection is an outbound switched call that attempts to remain up at all times. If the unit or central switch resets or if the link is terminated, the permanent switched connection attempts to restore the link at 10-second intervals, which is similar to the way a nailed connection is maintained. A permanent switch connection conserves connection attempts but causes a long connection time, which may be cost effective for some customers. For the answering device at the remote end of the permanent switched connection, we recommend that the Connection profile be configured to answer calls but not originate them, because if the remote device initiates a call, the DSL Terminator unit simply does not answer it. Continual call initiation could result in repeated charges for calls that have no purpose. To keep the remote device from originating calls, set AnsOrig to Ans Only for that device.

Example: `Call Type=Nailed`

Dependencies: A call type of Nailed makes parameters related to switched connections inapplicable, and a call type of Switched makes parameters related to nailed connections inapplicable.

Location: Ethernet > Connections > Telco Options, Ethernet > Frame Relay

See Also: AnsOrig, Backup, DLCI, FR DLCI, Group, Max Ch Count, Min Ch Count, Nailed Grp

Circuit

Description: Specifies an alphanumeric name for a DLCI endpoint. When combined as a circuit, the two DLCI endpoints act as a tunnel—data received on one DLCI bypasses the Lucent router and is sent out on the other DLCI.

A circuit is a permanent virtual circuit (PVC) segment that consists of two DLCI end points and possibly two Frame Relay profiles. It requires two and only two DLCI numbers: data is dropped if the circuit has only one DLCI and if more than two are defined, only two are used. Circuits are defined in two Connection profiles. Data coming in on the DLCI configured in the first Connection profile is switched to the DLCI configured in the second one.

Usage: Specify a name for the circuit, up to 16 characters. The other end-point of the PVC must specify the same name in its Circuit configuration.

Example: `Circuit=circuit-1`

Dependencies: This parameter applies only to FR_CIR-encapsulated calls.

Location: Ethernet > Connections > Encaps options

See Also: Encaps

Cir Timer

Description: Sets a ceiling to the Max Information Rate for circuits, including Frame Relay circuits and ATM Frame Relay circuits.

Usage: Enter a number in milliseconds between 10 and 5000. 5000 is the default.

Example: `Cir Timer=5000`

Location: Ethernet > Connections > Session Options

Client

Description: Enables the DSL Terminator unit to respond to multicast clients on the local Ethernet. Clients cannot be support on the MBONE interface, so this means that the multicast router resides across a WAN link.

Usage: Specify Yes or No.

- Yes means the DSL Terminator unit begins handling IGMP client requests and responses on the interface. It does not begin forwarding multicast traffic until the rate limit is set.

The Rate Limit parameter specifies the rate at which the DSL Terminator unit accepts multicast packets from its clients. It does not affect the MBONE interface.

- No means the DSL Terminator unit does not handle IGMP client requests and responses on the interface. No is the default.

Example: `Client=Yes`

Dependencies: This parameter is not applicable if Multicast Forwarding is disabled or if the local Ethernet is the MBONE interface (supporting a multicast router).

Location: Ethernet > Mod Config > Multicast

See Also: Multicast Forwarding, Mbone Profile

Client Assign DNS

Description: Specifies whether client DNS server addresses will be presented while this connection is being negotiated.

Usage: Specify Yes (to use client DNS servers) or No. No is the default.

Example: `Client Assign DNS = no`

Location: Ethernet > Connections > IP Options

See Also: Client Pri DNS, Client Sec DNS

Client Gateway

Description: Specifies a connection-specific default route to be used for forwarding packets received on this connection. The DSL Terminator unit uses this default route instead of the systemwide Default route in its routing table. This route is connection specific, so it is not added to the routing table.

Note: The DSL Terminator unit must have a direct route to the address you specify.

Usage: Specify the IP address of a next-hop router. The default value is 0.0.0.0; if you accept this value, the DSL Terminator unit routes packets as specified in the routing table, using the systemwide default route if it cannot find a more specific route.

Example: `Client Gateway=10.1.2.3`

Location: Ethernet > Connections > IP Options

Client Pri DNS

Description: Specifies a primary DNS server address to be sent to any client connecting to the DSL Terminator unit. Client DNS has two levels: a global configuration that applies to all PPP connections, and a connection-specific configuration that applies to that connection only. The global client addresses are used only if none are specified in the Connection profile. You can also choose to present your local DNS servers if no client servers are defined or available.

Usage: Specify the IP address of a DNS server to be used for all connections that do not have a DNS server defined. The default value is 0.0.0.0.

Example: `Client Pri DNS=10.9.8.7/24`

Location: Ethernet > Mod Config > DNS, Ethernet > Connections > IP Options

Client Sec DNS

Description: Specifies a secondary DNS server address to be sent to any client connecting to the DSL Terminator unit. Client DNS has two levels: a global configuration that applies to all PPP connections, and a connection-specific configuration that applies to that connection only. The global client addresses are used only if none are specified in the Connection profile. You can also choose to present your local DNS servers if no client servers are defined or available.

Usage: Specify the IP address of a secondary DNS server to be used for all connections that do not have a DNS server defined. The default value is 0.0.0.0.

Example: `Client Sec DNS=10.9.8.7/24`

Location: Ethernet > Mod Config > DNS, Ethernet > Connections > IP Options

Clock Source

Description: Specifies whether the T1 or E1 line may be used as the clock source for timing synchronous transmissions. If Clock Source is enabled, the line provides timing as long as it is active, is not in Red Alarm mode, and the DSL Terminator unit runs in recovered loop timing mode. If the DSL Terminator unit connects to more than one line, selecting Yes for each one gives the unit the option of using any of the lines as a source of synchronous timing.

Usage: Specify Yes or No.

- Yes means the line may be used as the clock source for timing synchronous transmissions. Yes is the default, and is the proper setting for normal operations.
- No means the line may not be used as the clock source. When this setting is No, the DSL Terminator unit uses another line for timing or uses its internal clock. This is recommended only when two DSL Terminator units connect to each other by a crossover cable (with optional T1 repeaters) between their network ports

Example: `Clock Source=Yes`

Location: Net/8T1 > Line Config > Line *N*, Net/8E1 > Line Config > Line *N*

See Also: Buildout, Encoding, Framing Mode, Front End, Length

Cold Start

Description: Specifies whether the system generates a trap when the DSL Terminator unit reinitializes itself so that the configuration of the SNMP manager or the system itself might be altered.

Usage: Specify Yes or No. The default is Yes.

- Yes specifies that the system generates a trap when the DSL Terminator unit reinitializes itself so that the configuration of the SNMP manager or the system itself might be altered.

- No specifies that the system does not generates a trap when the DSL Terminator unit reinitializes itself so that the configuration of the SNMP manager or the system itself might be altered.

Example: `Cold start=Yes`

Location: Ethernet > SNMP Traps > Enable Traps

See Also: Warm Start

Comm

Description: Specifies the SNMP community name associated with the SNMP Protocol Data Units (PDU). The string you specify becomes a password that the DSL Terminator unit sends to the SNMP manager when an SNMP trap event occurs. The password authenticates the sender identified by the host address.

Usage: Specify the community name, up to 31 characters. The default is *public*.

Example: `Comm=Lucent`

Dependencies: If this parameter and the Dest parameter are null, the DSL Terminator unit does not generate SNMP traps.

Location: Ethernet > SNMP Traps

See Also: Dest

Compare

Description: Specifies the type of comparison to make between the specified value in a filter and the specified location in the contents of a packet.

Usage: Specify one of the following values:

- Equals means the filter matches the packet when the specified value and the packet contents are equal. This is a default.
- NotEquals means the filter matches the packet when the specified value and the packet contents are equal.

Example: `Compare=Equals`

Dependencies: This parameter does not apply if the filter is not Valid or if the filter type is IP.

Location: Ethernet > Filters > Input filters > In filter *N* > Generic, Ethernet > Filters > Output filters > Out filter *N* > Generic

See Also: Length, Mask, Offset, Value, Valid

Compat Mode

Description: Enables or disables the Vendor-Specific Attribute (VSA) compatibility mode when the DSL Terminator unit is using RADIUS for call-logging to NavisAccess.

Usage: Specify one of the following settings:

- Old (the default) specifies that the DSL Terminator unit does not send the Vendor-Specific Attribute to the RADIUS server and does not recognize the Vendor-Specific Attribute if the server sends it.
- Vendor-Specific specifies that the DSL Terminator unit uses the Vendor-Specific Attribute to encapsulate Lucent vendor attributes, and uses the RFC-defined User-Password encryption algorithm as well.

Example: `Compat Mode=Old`

Location: Ethernet > Mod Config > Call Logging

See Also: Acct Compat Mode, Auth Compat Mode

Configuration Change

Description: Specifies whether the system generates a trap when a configuration is modified or a new image is loaded.

Usage: Specify Yes or No. The default is Yes.

- Yes specifies that the system generates a trap when a configuration is modified or a new image is loaded.
- No specifies that the system does not generates a trap when a configuration is modified or a new image is loaded.

Example: `Configuration Change=Yes`

Location: Ethernet > SNMP Traps > Enable Traps

Connection

Description: Specifies the number of a Connection profile needed to bring up a bridged or routed connection. The DSL Terminator unit uses this number to locate the profile and bring up the connection needed to forward packets whose destination address is not on the local network. If it receives a packet whose destination MAC address is not on the local Ethernet, it looks in the bridging table for a matching MAC address and uses the specified Connection profile to bring up a bridged connection.

Usage: Specify a Connection profile number.

Dependencies: Bridge profiles are not used for connections that enable dial-on-broadcast.

Example: `Connection #=2`

Location: Ethernet > Bridge Adrs

See Also: Dial Brdcast

Console

Description: In the System profile, specifies the interface established at the VT100 port labeled Control on the back panel of the DSL Terminator unit. In the SNMP Traps profile, specifies whether the system generates a trap when the console has changed state. The console entry can be read to see what its current state is.

Usage: In the System profile, specify one of the following values:

- Standard means the standard set of edit menus comes up in the VT100 window at system startup. This is the default.
- MIF means the Machine Interface Format (MIF) is accessible at system startup. From the MIF interface you can display the edit menus by pressing Ctrl-C and return to MIF again by using the Use MIF command.
- Limited means a set of simplified menus comes up. To enter or exit the simplified menus, press Ctrl-T.

In an SNMP Traps profile, specify Yes or No.

- Yes specifies that the system generates a trap when the console has changed state. The default is Yes.
- No specifies that the system does not generate a trap when the console has changed state.

Example: `Console=MIF`

Dependencies: You cannot operate MIF through a hand-held terminal. Only a VT100 terminal or emulator can operate MIF.

Location: Ethernet > SNMP Traps > Enable Traps, System > Sys Config

See Also: Ascend

Contact

Description: Specifies the person or department to contact to report error conditions. This field is SNMP readable and settable.

Usage: Specify the name of the contact person or department. You can enter up to 80 characters.

Example: `Contact=rchu`

Location: System > Sys Config

See Also: Location

D

Data Filter

Description: Specifies the number of a filter used to determine if packets should be forwarded or dropped. If both a call filter and data filter are applied to a connection, the DSL Terminator unit applies a call filter after applying a data filter. (Only those packets that the data filter forwards can reach the call filter.)

Usage: Specify a number between 0 and 199. The number you enter depends on the whether you are applying a filter you created using the VT100 interface, or a firewall you created using Secure Access Manager (SAM).

If you are applying a filter created using the VT100 interface, enter the last two digits of the filter number as it appears in the Filters menu.

If you are applying a firewall created with SAM, add 100 to the last two digits of the firewall number as it appears in the Firewalls menu. For example, if the number of your firewall is 90-601, specify 101. Refer to your SAM documentation for information on downloading firewalls to the DSL Terminator unit. The numbering scheme for filters and firewalls is:

- 0 indicates that no filtering is being used (this is the default)
- 1-99 indicates that a filter created using the VT100 interface is being used
- 100-199 indicates that a filter created using SAM is being used.

When you set Data Filter to 0 (zero), the DSL Terminator unit forwards all data packets.

Example: `Data Filter=7`

Location: Ethernet > Answer > Session Options, Ethernet > Connections > Session Options

See Also: Call Filter, Filter

Data Svc

Description: A data service is provided over a WAN line and is characterized by the unit measure of its bandwidth. A data service can transmit either data or digitized voice. In a Call profile, Connection profile, X.25, or Frame Relay profile, Data Svc specifies the type of data service the link uses. In a Dial Plan profile, Data Svc specifies the data service associated with the number the DSL Terminator dials under the extended dial plan.

Note: Either party can request a data service that is unavailable. In this case, the DSL Terminator cannot connect the call.

Usage: Specify one of the following values:

- 56K

  The call contains any type of data and connects to the Switched-56 data service. The only services available to lines using inband signaling (T1 or E1 lines containing one or more switched channels, and Switched-56 lines) are 56K and 56KR.
- 56KR

  The call contains restricted data, guaranteeing that the data the DSL Terminator transmits meets the density restrictions of D4-framed TI lines, and connects to the Switched-56 data

service. The only services available to lines using inband signaling (T1 or E1 lines containing one or more switched channels, and Switched-56 lines) are 56K and 56KR.

- 64K

  The call contains any type of data and connects to the Switched-64 data service. Data services above 64 kbps are not valid for a BONDING call.

- Voice (digital voice call)

  The call is an end-to-end digital voice call for transporting data when a switched data service is not available. If you choose this setting, the data may become unusable unless you meet these technical requirements:

  – Use only digital end-to-end connectivity; no analog signals should be present anywhere in the link.

  – Make sure that the phone company is not using any intervening loss plans to economize on voice calls.

  – Do not use echo cancellation; analog lines can echo, and the technology to take out the echoes can also scramble data in the link.

  – Do not make any modifications that can change the data in the link.

- Modem (digital modem call)

  The call uses a digital modem. If no digital modems are available, the call is not placed. The data rate depends upon the quality of the connections between modems and the types of modems used. This setting requires that your DSL Terminator have digital modems installed. Modem applies only when Encaps=MPP, PPP or X.25/PAD. Currently, multichannel modem calls are not supported even if Encaps=MPP.

- V.110 bit-rate data-service (V.110 terminal adapter call)

  The call uses a v.110 terminal adapter, using the PPP protocol at the specified bit rate over the specified data service line. The bit-rate may be one of the following:

  – 2.4

  – 4.8

  – 9.6

  – 19.2

  – 38.4

  The data-service may be one of the following:

  – 56K (switched-56)

  – 56KR (restricted switched-56)

  – 64K (switched-64)

  If the DSL Terminator cannot sync up with the remote terminal adapter using the specified bit rate, it attempts to use one of the other four bit rates.

- Inherit (use the data service requested by the local calling device)

  This setting is available only in Dial Plan profiles. The call connects with the data service as requested by the caller on the local Host/BRI line. If Data Svc is not set to Inherit in the Dial Plan profile, the setting in the Dial Plan profile overrides the settings in the Call profile and Connection profile.

- 384K/H0 (switched-384)

This setting is available only in Call profiles. It means that the call contains any type of data and connects to the Switched-384 data service. This AT&T data service does not require MultiRate or GloBanD. A Host/AIM6 expansion module supports a maximum of four 384K/H0 calls.

- 384KR (restricted switched-384)

  This setting is available only in Call profiles. It means that the call contains restricted data and connects to MultiRate or GloBanD data services at 384 kbps.

- 1536K (switched-1536)

  This setting is available only in Call profiles. It means that the call contains any type of data and connects to the Switched-1536 data service at 1536 kbps. This setting is valid only for lines using NFAS signaling.

- 1536KR (restricted switched-1536)

  This setting is available only in Call profiles. It means that the call contains restricted data and connects to the Switched-1536 data service at 1536 kbps. This setting is valid only for lines using NFAS signaling.

- 128K, 192K, 256K, and other multiples of 64K (multi-rate)

  This setting is available only in Call profiles. These values are available on a PRI line with MultiRate or GloBanD data services. If the DSL Terminator has the MultiRate option, these data services appear.

Example: `Data Svc=56K`

Dependencies: Because FT1 calls do not include switched services, the Data Svc parameter lists only 56KR and 64K when Call Type=FT1; in this context, the Data Svc setting indicates how much bandwidth the DSL Terminator routes to the host for each channel in the connection. When Call Type=FT1-B&O or Call Type=FT1-AIM, the Data Svc parameter refers to the switched channels.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > Telco Options, System > Dial Plan, Ethernet > Frame Relay, Ethernet > X.25

See Also: Call Type

Date

Description: Specifies the month, day, and year. You should set this parameter when installing the DSL Terminator unit.

Usage: Specify the current date in the format <month > /<day > /<year >. The default is 00/00/00.

Example: `Date=05/28/01`

Location: System > Sys Config

DBA Monitor

Description: Specifies how the DSL Terminator monitors the traffic over an MP+ connection. Only the initiating side of the call can add or subtract bandwidth. If both sides of the link have DBA Monitor set to None, Dynamic Bandwidth Allocation is disabled.

Usage: Usage: Specify one of the following values:

- `Transmit`—Specifies that the MAX adds or subtracts bandwidth based on the amount of data it transmits. Transmit is the default.
- `Transmit-Recv`—Specifies that the MAX adds or subtracts bandwidth based on the amount of data it transmits *and* receives.
- `None`—Specifies that the MAX does not monitor traffic over the link.

Example: `DBA Monitor=Transmit`

Dependencies: Dependencies: DBA Monitor is only supported on MP+ calls.

Location: Location: Ethernet > Connections > Encaps Options

See Also: See Also: Dyn Alg, Encaps, Idle Pct, Target Util

DCE N392

Description: Specifies the number of errors that causes the network side to declare the user side procedures inactive during DCE N393 monitored events.

Usage: Specify a value between 1 and 10 that is less than DCE N393.

Example: `DCE N392=3`

Dependencies: This parameter is N/A when FR Type is DTE.

Location: Ethernet > Frame Relay

See Also: DCE N393

DCE N393

Description: Specifies the DCE monitored event count (between 1 and 10).

Usage: Specify a value between 1 and 10 that is greater than DCE N392.

Example: `DCE N393=7`

Dependencies: This parameter is N/A when FR Type is DTE.

Location: Ethernet > Frame Relay

See Also: DCE 392

See Also:

Dec Ch Count

Description: Specifies the number of channels the DSL Terminator removes as a bundle when bandwidth changes either manually or automatically during a call. You cannot clear a call by decrementing channels. If the data service is 384K/H0 or 384KR, this value should be divisible by 6, because 384 kbps is 6x64 kbps. If the data service is MultiRate or GloBanD and the service you select is a multiple of 64 kbps, this value should be a multiple of 6.

Usage: Specify a number between 1 and 32. The default is 1.

Example: `Dec Ch Count=12`

Dependencies: This parameter does not apply if all channels of a link are nailed up. In a Call profile, this parameter applies only if the Call Type parameter is set to AIM, FT1-AIM, FT1-B& O, or BONDING and if Call Mgm parameter is set to Manual, Dynamic, or Mode 2.

Location: Location: Ethernet > Connections >Encaps Options

See Also: See Also: Base Ch Count, Inc Ch Count, Max Ch Count

Delay Dual

Description: Specifies whether the DSL Terminator inserts a ten-second delay between dialing the first and second calls in a dual-port call.

In a dual-port call, a codec performs inverse multiplexing on two channels so that a call can achieve twice the bandwidth of a single channel. Inverse multiplexing is a method of combining individually dialed channels into a single, higher-speed data stream.

The codec provides two ports, one for each channel. Two AIM ports on the DSL Terminator connect a dual-port call to the codec; these ports can be the V.35, RS-499, or X.21 ports on the DSL Terminator, and are called the primary port and the secondary port. Because the DSL Terminator places the two calls in tandem and clears the calls in tandem, it considers them a single call.

Usage: Specify Yes or No. No is the default.

- Yes specifies that the DSL Terminator waits ten seconds before dialing the second call in a dual-port call.
- No specifies that the DSL Terminator places both calls at the same time.

Example: `Delay Dual=Yes`

Location: System > Sys Config

Designate Egress

Description: Specifies the interface as an egress interface.

Usage: Specify Yes to designate an interface as an egress interface. The default value is No.

Example: `Designate Egress=Yes`

Dependencies: Connections must be configured for bridging or bridged IP routing, and CPE must be configured for bridging.

See Also: Ethernet > Connections > *any profile* > Bridge Options > Designate Egress

Dest

Description: In a Route profile, Dest specifies the route's target IP address. This is the destination address that causes the DSL Terminator unit to bring up this route. In a Route

profile, the default null address indicates the default route, used for all destinations that have no explicit route in the routing table.

In an SNMP Traps profile, Dest is the IP address to which the DSL Terminator unit sends traps (the IP address of the station running an SNMP management utility). The default null address means that no traps are sent. If the Comm parameter is also null, traps are turned off altogether.

Usage: Specify the destination IP address. The default value is 0.0.0.0/0.

Example: `Dest=10.207.23.1`

Dependencies: This parameter does not apply if the DSL Terminator unit does not support IP routing.

Location: Ethernet > Static Rtes, Ethernet > SNMP Traps

See Also: Gateway

Dest VRouter

Description: Specifies whether or not there is a static route between VRouters and, if there is, the name of the destination VRouter.

Usage: Specify the name of the destination VRouter. You can specify the main VRouter as the destination. The default is Dest Vrouter = 0.0.0.0, which specifies that this is not a static route between VRouters.

Example: `Dest VRouter=vr2`

Dependencies: The default setting of 0.0.0.0 is correct if the Gateway parameter, in the Static Rtes submenu, includes an IP address.

The Dest VRouter setting is valid only if the Sys Option Status display specifies `VRouter Avail`.

Location: Ethernet>Static Rtes>*any Static Rtes profile*

See Also: Active, Allow As Client DNS, Dest VRouter, Domain Name, Name, Pool#N Count, Pool#N Name, Pool#N Start, Pool Summary, Pri DNS,
RIP Policy, RIP Summary, RIP Trigger, Sec DNS, Sec Domain Name, VRouter IP Adrs

DHCP Client

Description: Specifies whether the DSL Terminator unit obtains its configuration parameters from a remote host using Dynamic Host Configuration Protocol (DHCP).

Usage: Specify Yes or No. The default is Yes.

Example: `DHCP Client=Yes`

Location: Ethernet > Mod Config

Dial

Description: Specifies the number used to dial out this connection.

Usage: Specify a phone number up to 24 characters. As an option, you can include a dialing prefix that directs the connection to use a trunk group. The DSL Terminator unit sends only the numeric characters to place a call. You must limit the number to these characters: 1234567890()[]!z-*#|

Example: `Dial #=6-1-808-555-1212`

Dependencies: This parameter is inapplicable for leased connections or connections using Frame Relay encapsulation.

Location: Ethernet > Connections, Ethernet > Frame Relay

See Also: Call Type, Encaps, Use Trunk Grps

Dial Brdcast

Description: Specifies whether the DSL Terminator unit dials this connection when it receives Ethernet broadcast packets. By default, the unit does not dialonbroadcast; it relies on its internal bridging table to bring up specific bridged connections.

If dial-on-broadcast is enabled in one or more Connection profiles, the DSL Terminator unit brings up all of those profiles whenever it receives Ethernet broadcast packets. It never uses a bridging table entry for those connections, even if one exists.

Usage: Specify Yes or No. No is the default.

- Yes means that the DSL Terminator unit dials this connection if it is not online and the unit receives a frame whose MAC address is set to broadcast.
- No specifies that broadcast packets do not cause the DSL Terminator unit to dial this connection.

Example: `Dial Brdcast=Yes`

Dependencies: This parameter applies only if the Connection profile enables bridging and allows outgoing calls.

Location: Ethernet > Connections

See Also: Connection #, Bridge, AnsOrig

Location:

Disc on Auth Timeout

Description: Specifies whether the DSL Terminator unit gracefully shuts down the PPP connection on an external authentication server timeout.

Usage: Specify Yes or No.

- Yes causes the DSL Terminator unit to hang up a PPP connection when an external authentication server times out.

- No causes the unit to shut down cleanly when the external authentication server request times out. No is the default.

Example: `Disc on Auth Timeout=Yes`

Dependencies: This parameter applies only to PPP connections.

Location: Ethernet > Answer > PPP Options

See Also: PPP

DLCI

Description: Specifies a Frame Relay DLCI number for a gateway or circuit connection. A DLCI is a number between 16 and 991, which is assigned by the Frame Relay administrator. A DLCI is not an address, but a local label that identifies a logical link between a device and a Frame Relay switch. The switch uses the DLCI to route frames through the network, and the DLCI may change as frames are passed through multiple switches.

The DSL Terminator unit receives an incoming PPP call, examines the destination address, and brings up the appropriate Connection profile to that destination, as usual. If the Connection profile specifies Frame Relay encapsulation, the Frame Relay profile, and a DLCI, the DSL Terminator unit encapsulates the packets in Frame Relay (RFC 1490) and forwards the data stream out to the Frame Relay switch using the specified DLCI. The Frame Relay switch uses the DLCI to route the frames. This is known as gateway mode.

Usage: Specify a number between 16 and 991. The default is 16. Ask your Frame Relay network administrator for the value you should enter.

Example: `DLCI=17`

Dependencies: This parameter applies only to FR and FR_CIR encapsulated calls.

Location: Ethernet > Connections > Encaps Options, Ethernet > Connections > Session Options

See Also: Encaps, FR Direct, FR DLCI

DM

Description: Specifies the subaddress associated with the DSL Terminator unit's digital modems. The DSL Terminator routes an incoming call whose subaddress matches the value of DM to the first available digital modem; the DSL Terminator handles such a call as a terminal server call. If the subaddress matches DM, but no digital modem is available, the DSL Terminator clears the call.

Usage: Specify a subaddress. You can specify a number between 0 and 99. The default is 0.

Dependencies: This parameter is ignored if the Sub-Adr parameter is not set to Routing.

Location: System > Sys Config

See Also: Ans *N*#, Sub-Adr

Domain Name

Description: Specifies the local DNS domain name. The domain name is used for DNS lookups. When the DSL Terminator unit is given a hostname to look up, it tries various combinations including appending the configured domain name. The secondary domain name (Sec Domain Name) can specify another domain name that the unit can search using DNS.

Usage: Specify the domain name of the DSL Terminator unit. You can enter up to 63 characters.

Example: `Domain Name=mydomain`

Location: Ethernet > Mod Config > DNS

See Also: Pri DNS, Sec DNS, Sec Domain Name

Download

Description: Enables or disables permission to download the configuration of the DSL Terminator unit using the Save Cfg parameter. Passwords are not saved to file.

Note: Passwords are not saved when you download the configuration. If you upload a saved configuration, all passwords are wiped out.

Usage: Specify Yes or No. No is the default.

- Yes means the operator can download the DSL Terminator configuration (without the password values) by using the Save Cfg command in the Sys Diag menu.
- No disables this permission.

Example: `Download=Yes`

Dependencies: This parameter is not applicable if the Operations permission is disabled.

Location: System > Security

DownMetric

Description: This parameter specifies the metric for a route whose associated WAN connection is down.

Usage: Specify an integer. The higher the metric, the less likely that the DSL Terminator unit will use the route. The default metric for online WAN connections is 1. The default metric for offline WAN connections is 7. The metric you specify is in effect only as long as the WAN connection is down

Example: `DownMetric=2`.

Location: Ethernet > Static Rtes

See Also: DownPreference

DownPreference

Description: This parameter specifies the preference value for a route whose associated WAN connection is down.

Usage: Specify an integer. A higher preference number represents a less desirable route. The default preference for online WAN connections is 60. The default preference for offline WAN connections is 120. The preference you specify is in effect only as long as the WAN connection is down.

Example: `DownPreference=65`

Dependencies: Make sure that routes for offline connections have a higher preference number than routes for online connections. The following table lists the factory default values for route preferences.

Route type	Default value
Interface	0
ICMP	30
RIP	100
OSPF ASE	150
OSPF Internal	10
Static	60
Down-Wan	120
Infinite	225

Location: Ethernet > Static Rtes

See Also: DownMetric

DS0 Min Rst

Description: 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.

A DS0 minute is the online usage of a single 56-kbps or 64-kbps switched channel for one minute. When the usage exceeds the maximum specified by the Max DS0 Mins parameter, the DSL Terminator cannot place any more calls, and takes any existing calls offline.

In a System profile, the accumulated minutes apply to all ports on the DSL Terminator and to the Ethernet module. In a Port profile, the accumulated minutes apply only to the associated AIM port.

Usage: Specify one of the following values:

- Daily specifies that the DSL Terminator resets the accumulated DS0 minutes to 0 (zero) every day at 12 A.M.
- Monthly specifies that the DSL Terminator resets the accumulated DS0 minutes to 0 (zero) on the first day of every month at 12 A.M.

- Off (the default) specifies that the DSL Terminator disables the Max DS0 Mins parameter in the System profile or Port profile.

Example: `DS0 Min Rst`

Location: System > Sys Config

See Also: Max Call Mins, Max DS0 Mins

Dst Adrs

Description: Specifies a destination IP address. After this value has been modified by applying the specified Dst Mask, it is compared to a packet's destination address.

Usage: Specify a destination IP address the DSL Terminator unit should use for comparison when filtering a packet. The zero address 0.0.0.0 is the default. If you accept the default, the unit does not use the destination address as a filtering criterion.

Example: `Dst Adrs=10.62.201.56`

Dependencies: This parameter applies only to filters of type IP.

Location: Ethernet > Filters > Input filters > In filter *N* > IP, Ethernet > Filters > Output filters > Out filter *N* > IP, Ethernet > Filters > Input filters > In filter *N* > IPTOS, Ethernet > Filters > Output filters > Out filter *N* > IPTOS

See Also: Dst Mask

Dst Mask

Description: Specifies a mask to apply to the Dst Adrs before comparing it to the destination address in a packet. You can use it to mask out the host portion of an address, for example, or the host and subnet portion.

The DSL Terminator unit applies the mask to the address using a logical AND after the mask and address are both translated into binary format. The mask hides the portion of the address that appears behind each binary 0 (zero) in the mask. A mask of all zeros (the default) masks all bits, so all destination addresses are matched. A mask of all ones (255.255.255.255) masks no bits, so the full destination address to a single host is matched.

Usage: Specify the mask in dotted decimal format. The zero address 0.0.0.0 is the default; this setting indicates that the DSL Terminator unit masks all bits. To specify a single destination address, set Dst Mask=255.255.255.255 and set Dst Adrs to the IP address that the DSL Terminator unit uses for comparison.

Example: `Dst Mask=255.255.255.0`

Dependencies: This parameter applies only to filters of type IP.

Location: Ethernet > Filters > Input filters > In filter *N* > IP, Ethernet > Filters > Output filters > Out filter *N* > IP, Ethernet > Filters > Input filters > In filter *N* > IPTOS, Ethernet > Filters > Output filters > Out filter *N* > IPTOS

See Also: Dst Adrs

Dst Port

Description: Specifies the UDP destination port to use for call-logging requests.

Usage: Specify a UDP port number from 1 to 32767. The value must match the port number configured on the call-logging host. The default of 0 (zero) indicates any UDP port.

Example: `Dst Port=1260`

Dependencies: If Call Log=No, Dst Port does not apply.

Location: Ethernet > Mod Config > Call Logging

See Also: Acct-ID Base, Allow Stop Only, Call Log, Call Log Timeout, Host # N, Key, Max Retry, Reset Timeout

Dst Port

Description: In a filter, specifies a value to compare with the destination port number in a packet. In a Network Address Translation (NAT) for LAN static mapping, the Dst Port # parameter specifies a TCP or UDP port that users outside the private network can access. The DSL Terminator unit can route packets for this port to a specific server and port on the local network. This routing, which occurs only in conjunction with Network Address Translation (NAT), is controlled by the parameters in the Static Mapping *N* submenu.

Note: If you change the value of Dst Port # or of any of the other parameters in a Static Mapping *N* submenu, the change does not take effect until the next time a connection is made to the remote network. To make the change immediately, you must terminate the connection to the remote network and then reopen it.

Usage: Specify the number of the destination port. You can enter a number between 0 and 65535. The default setting is 0 (zero), which disables the use of a destination port. Port 25 is reserved for SMTP; that socket is dedicated to receiving mail messages. Port 20 is reserved for FTP data messages, port 21 for FTP control sessions, and port 23 for telnet.

Example: `Dst Port #=25`

Dependencies: Keep this additional information in mind:

- In a Filter profile, Dst Port # applies to filters of type IP.
- The Protocol parameter in the Static Mapping *N* submenu determines whether the port you specify is a TCP or UDP port. For routing of incoming packets for a particular port to occur, the following conditions must be met:
  - The Routing parameter must be set to Yes.
  - The Lan parameter must be set to Single IP Addr.
  - The Valid parameter must be set to Yes.
  - The Dst Port # and Loc Port # parameters must be set to a value other than 0 (zero).
  - The Loc Addr parameter must be set to an address other than 0.0.0.0.

Location: Ethernet > Filters > Input filters > In filter *N* > IP,
Ethernet > Filters > Output filters > Out filter *N* > IP,
Ethernet > Filters > Input filters > In filter *N* > IPTOS,

Ethernet > Filters > Output filters > Out filter *N* > IPTOS,

See Also: Dst Port Cmp, Loc Port #, Src Port Cmp, Src Port #

Dst Port Cmp

Description: Specifies the type of comparison the DSL Terminator unit makes when using the Dst Port # parameter.

Usage: Specify one of the following values:

- None specifies that the DSL Terminator unit does not compare the packet's destination port to the value specified by Dst Port #. None is the default.
- Less specifies that port numbers with a value less than the value specified by Dst Port # match the filter.
- Eql specifies that port numbers equal to the value specified by Dst Port # match the filter.
- Gtr specifies that port numbers with a value greater than the value specified by Dst Port # match the filter.
- Neq specifies that port numbers not equal to the value specified by Dst Port # match the filter.

Example: `Dst Port Cmp=None`

Dependencies: This parameter works only for TCP and UDP packets. You must set it to None if the Protocol parameter is not set to 6 (TCP) or 17 (UDP).

Location: Ethernet > Filters > Input filters > In filter *N* > IP, Ethernet > Filters > Output filters > Out filter *N* > IP, Ethernet > Filters > Input filters > In filter *N* > IPTOS, Ethernet > Filters > Output filters > Out filter *N* > IPTOS

See Also: Dst Port #

DTE N392

Description: Specifies the number of errors during DTE N393 monitored events which cause the user side to declare the network side procedures inactive.

Usage: Specify a value between 1 and 10 that is less than DTE N393.

Example: `DTE N392=3`

Dependencies: This parameter is N/A when FR Type is DCE.

Location: Ethernet > Frame Relay

See Also: DTE N393

DTE N393

Description: Specifies the DTE monitored event count (between 1 and 10). It is N/A when FR Type is DCE.

Usage: Specify a value between 1 and 10 that is greater than DTE N392.

Example: `DTE N393=5`

Dependencies: This parameter is N/A when FR Type is DCE.

Location: Ethernet > Frame Relay

See Also: DTE N392

Dyn Alg

Description: Specifies an algorithm for calculating average line utilization (ALU) over a certain number of seconds (Sec History).

Usage: Specify one of the following values:

- Quadratic (the default) gives more weight to recent samples of bandwidth usage than to older samples taken over the specified number of seconds. The weighting grows at a quadratic rate.
- Linear gives more weight to recent samples of bandwidth usage than to older samples taken over the specified number of seconds. The weighting grows at a linear rate.
- Constant gives equal weight to all samples taken over the specified number of seconds.

Example: `Dyn Alg=Quadratic`

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options

See Also: Add Pers, Dec Ch Count, Dyn Alg, Inc Ch Count, Max Ch Count, Sec History, SubPers, Target Util

E

Edit

Description: Enables you to customize which status windows are displayed in the VT100 interface at system startup.

Usage: Specify a slot and port address using the format XY-NNN.

- X is the slot number. The system itself is assigned slot number 0 (00-000).
- *Y* is the port number. Zero means any port on the slot.
- The three digits after the dash are the root number. A root number of 000 identifies a top-level branch of the menu tree. If *N* is not zero, the root number identifies a submenu.

Example: `Edit=00-000`

Location: System > Sys Config

Edit All Calls

Description: Enables or disables permission to edit all the parameters in all Call profiles and Connection profiles. When the permission is disabled, the operator is restricted to editing only the Dial # and Base Ch Count parameters in the current Call profile. The operator may access the profiles via Telnet, by local management, or by remote management.

Note: To restrict editing entirely, you must also disable the Edit Cur Call permission.

Usage: Specify Yes or No. Yes is the default.

- Yes means the operator can edit all parameters in Call and Connection profiles. Yes is the default.
- No means the operator can edit only the Dial # and Base Ch Count parameters in the current Call profile.

Example: `Edit All Calls=Yes`

Dependencies: This parameter does not apply if the Operations permission is disabled.

Location: System > Security

See Also: Edit Com Call, Edit Cur Call, Edit Own Call

Edit All Ports

Description: Enables or disables permission to edit all Port profiles. When the permission is disabled, the operator is restricted to editing only the current Port profile. The operator may access the profiles via Telnet, by local management, or by remote management.

Note: To restrict editing Port profiles entirely, you must also disable the Edit Own Port permission.

Usage: Specify Yes or No.

- Yes means the operator can edit all Port profiles. Yes is the default.

- No means the operator can edit only the current Port profile.

Example: `Edit All Ports=Yes`

Dependencies: This parameter does not apply if the Operations permission is disabled.

Location: System > Security

See Also: Edit Own Port

Edit Com Call

Description: Specifies whether an operator can edit Call profiles that are not specific to any AIM port. These profiles are known as common Call profiles. Numbers 201 through 216 denote port-specific Call profiles. Numbers 217 through 232 denote common Call profiles. The operator may access the profiles via Telnet, by local management, or by remote management.

Note: To restrict editing common Call profiles entirely, you must also disable the Edit All Calls permission.

Usage: Specify Yes or No.

- Yes means the operator can edit Call profiles that are not specific to any AIM port (common Call profiles). Yes is the default if Edit All Calls is set to No.
- No disables this permission.

Example: Edit Com Calls=Yes

Dependencies: This parameter does not apply if the Operations permission is disabled or the Edit All Calls permission is set to Yes.

Location: System > Security

See Also: Edit All Calls

Edit Cur Call

Description: Specifies whether an operator can edit all the parameters in the current Call profile. When the permission is disabled, the operator is restricted to editing only the Dial # and Base Ch Count parameters in the current Call profile. The operator may access the profiles via Telnet, by local management, or by remote management.

Note: To restrict editing entirely, you must also disable the Edit All Calls permission.

Usage: Specify Yes or No. Yes is the default if Edit All Calls is set to No.

- Yes means the operator can edit Call profiles that are not specific to any AIM port (common Call profiles).
- No disables this permission.

Example: `Edit Cur Calls=Yes`

Dependencies: This parameter does not apply if the Operations permission is disabled or the Edit All Calls permission is set to Yes.

Location: System > Security

See Also: Edit All Calls

Edit Line

Description: Specifies whether an operator can edit Line profiles.

Usage: Specify Yes or No. No is the default.

- Yes means the operator can edit all Line profiles.
- No means the operator can edit only the current Line profile.

Example: `Edit Line=Yes`

Dependencies: This parameter does not apply if the Operations permission is disabled.

Location: System > Security

Edit Own Call

Description: Specifies whether an operator can edit the Call profile for the port that has been called. The operator may access the profiles via Telnet, by local management, or by remote management.

Note: To restrict editing entirely, you must also disable the Edit All Calls permission.

Usage: Specify Yes or No. Yes is the default if Edit All Calls is set to No.

- Yes means the operator can edit the Call profile for the port that has been called.
- No disables this permission.

Example: `Edit Own Call=Yes`

Dependencies: This parameter does not apply if the Operations permission is disabled or the Edit All Calls permission is set to Yes.

Location: System > Security

See Also: Edit All Calls

Edit Own Port

Description: Enables or disables permission to edit the Port profile for the port that has been called.

Note: To restrict editing Port profiles entirely, you must also disable Edit All Port.

Usage: Specify Yes or No.

- Yes means the operator can edit the Port profile for the port that has been called. Yes is the default if Edit All Ports is set to No.
- No disables this permission.

Example: `Edit Own Port=Yes`

Dependencies: This parameter does not apply if the Operations permission is disabled or the Edit All Ports permission is set to Yes.

Location: System > Security

See Also: Edit All Ports

Edit Security

Description: Enables or disables permission to edit Security profiles.

Note: Do not set the Edit Security parameter to No in all Security profiles; if you do, you will be unable to edit any of them. This is the most powerful security permission because it gives the operator the ability to modify his or her own permissions.

Usage: Specify Yes or No.

- Yes means the operator can edit Security profiles. Yes is the default.
- No means the operator cannot edit Security profiles.

Example: `Edit Security=Yes`

Dependencies: This parameter does not apply if the Operations permission is disabled.

Location: System > Security

Edit System

Description: Enables or disables permission to edit the System profile and the Read Comm and R/W Comm parameters in the Ethernet profile.

Usage: Specify Yes or No.

- Yes means the operator can edit the System profile and SNMP community strings.Yes is the default.
- No disables this permission.

Example: `Edit System=Yes`

Dependencies: This parameter does not apply if the Operations permission is disabled.

Location: System > Security

Enable

Description: Enables FRF.5 internetworking for the Frame Relay profile.

Usage: Specify Yes or No. the default is No.

Example: `Enable=Yes`

Location: Ethernet > Frame Relay > *Frame Relay profile* >FRF.5 Options

See Also: VPI, VCI, Traffic Shaper

Enabled

Description: Enables a Traffic Shaper profile.

Usage: Specify one of the following values.

- No (the default) specifies the Traffic Shaper profile is not enabled.
- Yes specifies the Traffic Shaper profile is enabled.

Example: `Enabled=Yes`

Location: Net/DS3-ATM > Line Config > *any line profile* > Traffic Shapers,
Net/OC3-SMF-ATM > Line Config > *any line profile* > Traffic Shapers,
Net/OC3-UTP-ATM > Line Config > *any line profile* > Traffic Shapers

See Also: Aggregate, Bit Rate, Max Burst Size, Peak Rate, Priority, Traffic Shaper

Enabled (BIR)

Description: Enables or disables bridged IP routing (BIR).

Usage: Specify Yes or No.

- Yes enables BIR for the Connection profile.
- No disables BIR for the Connection profile. No is the default.

Example: `Enabled=Yes`

Dependencies: Enabled does not apply if Route IP is set to No in the Connection profile.

Location: Ethernet > Connections > *any Connection profile* > BIR options

See Also: Bridge Group, Proxy ARP

Encaps

Description: Specifies the encapsulation method to use when exchanging data with a remote network. Both sides of the link must use the same encapsulation for the connection to be established.

Note: When you specify an encapsulation method, the Encaps Options submenu displays a group of parameters relevant to your selection; you must set the appropriate Encaps Options parameters.

Usage: Specify one of the following values:

- PPP (Point-to-Point Protocol) for standard PPP
- MP (Multilink PPP)
- MPP (Multilink Protocol Plus)
- FR (Frame Relay)
- FR_CIR (Frame relay circuit)
- ARA (AppleTalk Remote Access client dialins)

Example: `Encaps=MPP`

Dependencies: The encapsulation type must be enabled in the Answer profile.

Location: Ethernet > Connections

See Also: FR, MP, MPP, PPP

Encoding

Description: Sets the layer-1 line encoding to use for the physical link. The Encoding value refers to the way in which data is represented by the digital signals on the line. Both sender and receiver must agree on the type of encoding in use in order to accurately interpret the value of a signal.

Usage: Specify one of the following values:

- AMI (the default) specifies Alternate Mark Inversion encoding.
- B8ZS specifies Bipolar encoding with 8-Zero Substitution.

Example: `Encoding=B8ZS`

Location: Net/8T1 > Line Config > Line *N*

See Also: Buildout, Clock Source, Framing Mode, Front End, Length

Enet Adrs

Description: In a Bridge profile, specifies the physical Ethernet address (MAC address) of a device at the remote end of the link. The Bridge profile correlates a remote MAC address with a Connection profile number, enabling the DSL Terminator unit to bring up that Connection when it receives packets destined for the remote device.

Usage: Specify the physical address of the device on the remote network. An Ethernet address is a 12-digit hexadecimal number. The default setting is 000000000000.

Example: `Enet Adrs=0180C2000000`

Location: Ethernet > Bridge Adrs

See Also: Net Adrs

Event Overwrite

Description: Specifies whether the system generates a trap when a new event has overwritten an unread event. This trap is sent only for systems that support Lucent's accounting MIB. Once sent, additional overwrites will not cause another trap to be sent until at least one table's worth of new events have occurred.

Usage: Specify Yes or No.

- Yes specifies that the system generates a trap when a new event has overwritten an unread event. The default is Yes.
- No specifies that the system does not generate a trap when a new event has overwritten an unread event.

Example: `Event Overwrite=Yes`

Location: Ethernet > SNMP Traps > Enable Traps

See Also: Configuration Change

Excl Routing

Description: Enables or disables exclusive port routing. Exclusive port routing is a way to prevent the DSL Terminator from accepting calls for which it has no explicit routing destination. If Excl Routing is disabled (the default), the call is routed to a digital modem if the bearer service is voice. If the service is V.110, it is routed to the first available V.110 module. If the service is data, it is routed to the first available AIM port; or if no AIM ports are available, it is routed to the DSL Terminator unit's bridge/router. To prevent this service-based routing and instead reject the call, turn Excl Routing on.

Usage: Specify Yes or No.

- Yes means the DSL Terminator drops calls for which it has no explicit call-routing information (such as Answer numbers, ISDN subaddressing, and so forth).
- No means the DSL Terminator uses service-based routing to route voice calls to a digital modem and data calls to an AIM port or its bridge/router software. No is the default.

Note: With MAXPOTS functionality, the default for Excl Routing is Yes.

Example: `Excl Routing=No`

Location: System > Sys Config

Exp Callback

Description: Specifies whether the DSL Terminator expects outgoing calls to result in a call back from the far end device. Use this parameter when the remote device requires callback security.

Usage: Specify Yes or No.

- Yes means the DSL Terminator expects the connection to terminate and result in a call-back from the far end device. This prevents problems that arise when CLID is set to Required on the device that is expected to callback. If a call fails for any reason, regardless of whether or not the called machine requires CLID and is attempting a callback, the call initiator will still have to wait 90 seconds before attempting the call the same number again if Exp Callback is set to Yes.
- No means the DSL Terminator does not expect call-back for this connection. No is the default.

Example: `Exp Callback=No`

Location: Ethernet > Connections > Telco Options

See Also: CallbackExtlink

Description: Specifies a link to an extension firewall profile. The value of Extlink lets you know that the firewall is large enough to require an extension profile.

Usage: The Extlink value is read only.

Location: Ethernet > Firewalls

See Also: Version

F

FDL

Description: Specifies the Facilities Data Link (FDL) protocol that the DSL Terminator unit uses. FDL is a protocol used by the telephone company to monitor the quality and performance of T1 lines. It provides information at regular intervals to your carrier's maintenance devices.

You continue to accumulate D4 and ESF performance statistics in the FDL Stats windows, even if you do not choose an FDL protocol. Your carrier can tell you which FDL protocol to specify.

Usage: Specify one of the following values:

- None (the default) disables FDL signaling.
- AT&T specifies AT&T FDL signaling.
- ANSI specifies ANSI FDL signaling.
- Sprint specifies Sprint FDL signaling.

Example: `FDL=None`

Dependencies: This parameter does not apply to D4-framed T1 lines.

Location: Net/8T1 > Line Config > Line *N*

See Also: Framing Mode

Field Service

Description: Enables or disables permission to perform Lucent-provided field service operations, such as uploading new system software. Field service operations are special diagnostic routines not available through the unit's menus.

Usage: Specify Yes or No.

- Yes means the operator can upgrade the system software and perform other field service operations. Yes is the default.
- No disables this permission.

Example: `Field Service=No`

Dependencies: This parameter is not applicable if the Operations permission is disabled.

Location: System > Security

Filter

Description: Specifies the number of a data filter that plugs into the Ethernet profile. The data filter manages data flow on the Ethernet interface. The filter examines each incoming or outgoing packet and uses the Forward parameter setting to determine whether to forward or discard.

Usage: Specify a number between 0 and 199. The number you enter depends on whether you are applying a filter you created using the VT100 interface or a firewall you created using Secure Access Manager (SAM).

If you are applying a filter created using the VT100 interface, enter the last two digits of the filter number as it appears in the Filters menu.

If you are applying a firewall created with SAM, add 100 to the last 2 digits of the firewall number as it appears in the Firewalls menu. For example, if the number of your firewall is 90-601, specify 101. Refer to your SAM documentation for information on downloading firewalls to the DSL Terminator unit. The numbering scheme for filters and firewalls is as follows:

- 0 indicates that no filtering is being used (this is the default)
- 1-99 indicates that a filter created using the VT100 interface is being used
- 100-199 indicates that a firewall created using SAM is being used.

When you set Filter to 0 (zero), the DSL Terminator unit forwards all data packets.

Example: `Filter=7`

Location: Ethernet > Mod Config > Ether Options

See Also: Call Filter, Data Filter

Filter Persistence

Description: Specifies whether the filter or firewall assigned to a Connection profile should persist after the call has been disconnected. Before Secure Access was supported, the DSL Terminator unit simply constructed a filter on a WAN interface when the connection was established and destroyed the filter when the connection was brought down, even if the connection just timed out momentarily. This works fine for static packet filters, but does not accommodate Secure Access firewalls. The Filter Persistence parameter is needed to allow firewalls to persist across connection state changes, but it is not needed for filters. If you do set it for a static packet filter, the filter persists across connection state changes.

Note: Firewalls must have persistence to work correctly; filters do not need persistence.

Usage: Specify Yes or No.

- Yes causes the filter or firewall to persist across connection state changes. This is not required for a data or call filter, but it is required for firewalls.
- No causes the filter or firewall to be torn down when a connection is brought down. No is the default.

Example: `Filter Persistence=Yes`

Location: Ethernet > Answer > Session options, Ethernet > Connections > Session options

See Also: Call Filter, Data Filter, Name, Version, Length

Finger

Description: Enables or disables the Finger remote user information protocol (RFC 1288). Finger returns information about users currently logged into the DSL Terminator unit. Note that for security reasons, the unit does not forward Finger requests.

Usage: Specify one of the following values:

- Yes enables the DSL Terminator unit to respond to Finger requests.
- No disables the Finger protocol on the DSL Terminator unit.

Example: `Finger=Yes`

Location: Ethernet > Mod Config

First DS0 Channel

Description: Specifies the first DS0 for the nailed T1 or EI line. Get this information from your WAN service provider.

Usage: Specify the first DS0. You can specify a number between 1 and 24 (for T1) or 1 and 32 (for E1).

Example: `First DS0 Channel=3`

Dependencies: First DS0 Channel must be set to a value less than the Last DS0 Channel value.

Location: Net/8T1 > Line Config > Line *N*, Net/8E1 > Line Config > Line *N*

See Also: Last DS0 Channel

Force 56

Description: Specifies whether the DSL Terminator uses only the 56Kbps portion of a channel, even when all 64 Kbps appear to be available. Use this feature when you receive calls from European or Pacific Rim countries and the complete path cannot distinguish between the Switched-56 and Switched-64 data services. This feature is not required if you are receiving calls only from North America.

Note: The DSL Terminator uses the Force 56 value in a Connection profile only if the call authenticates by means of CLID/DNIS. The DSL Terminator uses the Force 56 value in the Answer profile if a call authenticates by means of name and password, or for unauthenticated calls.

Usage: Specify Yes or No.

- Yes means the DSL Terminator uses 56K of a channel that may provide up to 64K bandwidth.
- No means the DSL Terminator uses the full 64K bandwidth if it is available. No is the default.

Example: `Force 56=Yes`

Dependencies: This parameter should not be enabled for calls within North America.

Location: Ethernet > Connections >Telco Options, Ethernet > Answer

Force Fragmentation

Description: Specifies whether or not the DSL Terminator unit prefragments incoming packets that have the Don't Fragment (DF) bit set, when the packets are larger than the negotiated Maximum Receive Unit (MRU).

Usage: Specify Yes or No.

- Yes specifies that the DSL Terminator unit ignores the DF bit and performs the fragmentation that normally should be performed by the client. It prefragments those packets at the specified GRE MTU size, and then adds the GRE and IP headers.

  Setting the Force Fragmentation setting to Yes causes the DSL Terminator unit to bypass the standard MTU discovery mechanism and fragment larger packets before encapsulating them in GRE. Because this scenario changes expected behavior, it is not recommended except for ATMP interoperation with outdated client software that does not handle fragmentation properly.
- No (the default) specifies that the DSL Terminator unit does not fragment an incoming packet that has the DF bit set. No is the default.

Example: `Force Fragmentation=Yes`

Dependencies: You must set GRE MTU to a nonzero value for a setting of Force Fragmentation=Yes to have any effect.

Location: Ethernet > Mod Config > ATMP Options

See Also: GRE MTU

Forward

Description: Specifies whether the DSL Terminator unit discards or forwards packets that match the filter specification. When no filters are in use, the unit forwards all packets by default. When a filter is in use, the default is to discard matching packets (Forward=No).

Usage: Specify Yes or No.

- Yes means the DSL Terminator unit forwards packets that match the filter.
- No means the DSL Terminator unit discards packets that match the filter. No is the default.

Example: `Forward=No`

Location: Ethernet > Filters > Input filters > In filter *N* > IP, Ethernet > Filters > Output filters > Out filter *N* > IP

See Also: Call Filter, Data Filter, Filter, More

Forwarding

Description: Enables multicast forwarding in the DSL Terminator unit.

Note: When you change the Forwarding parameter from No to Yes, the multicast subsystem reads the values in the Ethernet profile and initiates the forwarding function. If you modify a multicast value in the Ethernet profile, you must set this parameter to No and then set it to Yes again to force a read of the new value.

Usage: Specify Yes or No.

- Yes turns on multicast forwarding.
- No disables multicast forwarding. No is the default

Example: `Forwarding=Yes`

Location: Ethernet > Mod Config > Multicast

See Also: Mbone Profile, Multicast Client

Forward Directed Bcast

Description: Specifies whether the DSL Terminator unit responds to directed-broadcast ICMP echo requests.

Usage: Specify Yes or No.

- Yes directs the DSL Terminator unit to respond to directed broadcast ICMP echo requests. Yes is the default.
- No directs the DSL Terminator unit not to respond to directed broadcast ICMP echo requests.

Example: `Forward Directed Bcast=Yes`

Dependencies: Forward Directed Bcast applies only if the DSL Terminator unit supports IP routing.

Location: Ethernet > Mod Config

See Also: Reply DirectedBcast Ping

FR

Description: Specifies whether the DSL Terminator unit accepts incoming Frame Relay-encapsulated calls.

Usage: Specify Yes or No.

- Yes means the unit accepts calls that use Frame Relay encapsulation, provided that they meet all other connection criteria. Yes is the default.
- No means the unit will not accept inbound calls using Frame Relay encapsulation.

Example: `FR=Yes`

Location: Ethernet > Answer > Encaps

See Also: Encaps, FR Prof, DLCI

Framed Addr Start

Description: Specifies whether to send a second RADIUS Accounting Start record when the RADIUS Framed-Address value is assigned.

Usage: Specify Yes or No.

- Yes enables the DSL Terminator unit to send a second RADIUS Accounting Start record when the RADIUS Framed-Address value is assigned.
- No prevents the DSL Terminator unit from sending a second RADIUS Accounting Start record. The default is No.

Example: `Framed Add Striates`

Location: Ethernet > Mod Config > Auth

Framing Mode

Description: Specifies the framing mode the T1 or E1 physical layer uses. Your carrier can tell you which framing mode to choose.

Usage: Specify one of the following values for a Net/8T1 line:

- D4 specifies the D4 format, also known as the Superframe format. This format consists of 12 consecutive frames, separated by framing bits.
- ESF specifies the Extended Superframe Format. This format consists of 24 consecutive frames, separated by framing bits.

For a Net/8E1 line, specify one of the following values:

- G.703 (the default) specifies standard framing mode.
- 2DS specifies a variant of G.703.

Example: `Framing Madhouses`

Location: Net/8T1 > Line Config > Line *N*, Net/8E1 > Line Config > Line *N*

See Also: Bulldog, Clock Source, Encoding, Front End, Length

FR Circuit

Description: Specifies a name for a Data Link Connection Indicator (DLCI) endpoint.

Usage: Specify a name for the circuit. You may enter up to 16 characters. The other endpoint of the Permanent Virtual Connection (PVC) must specify the same name in its circuit configuration.

Example: `FR Circuit=ZZBON2`

Dependencies: FR Circuit applies only to gateway or circuit connections.

Location: Ethernet > Connections > Uncaps Options

FR Direct

Description: Specifies whether the DSL Terminator redirects incoming packets to the Frame Relay switch without processing. A FR Direct connection is a dial-in IP routing connection (typically using PPP), for which the DSL Terminator unit simply forwards the packets automatically to the Frame Relay switch without examining destination addresses or its routing table. In effect, the unit passes on the responsibility of routing those packets to a later hop on the Frame Relay network. This is known as FR Direct mode and is not commonly used.

Note: A FR Direct connection is not a full-duplex tunnel between the PPP dial-in and the switch. The IP packets coming back from the Frame Relay switch are handled by the DSL Terminator unit router software, so they must contain the PPP caller's IP address to be routed correctly back across the WAN.

Usage: Specify Yes or No. No is the default.

- Yes means this connection is a FR Direct connection.
- No means this is not a FR Direct connection.

Example: `Framed Directs`

Dependencies: This parameter is not applicable for FR or FR_CIR encapsulated calls.

Location: Ethernet > Connections > Session Options

See Also: FR DLCI, FR Prof

FR DLCI

Description: Specifies a Frame Relay DLCI number to be used for FR Direct connections. A FR Direct connection is a dial-in IP routing connection (typically using PPP), for which the DSL Terminator unit simply forwards the packets automatically to the Frame Relay switch without examining destination addresses or its routing table. In effect, the unit passes on the responsibility of routing those packets to a later hop on the Frame Relay network. This is known as FR Direct mode, and is not commonly used.

Note: More than one FR Direct PPP connection can share a Frame Relay DLCI.

Usage: Specify the DLCI obtained from the Frame Relay administrator for FR Direct links.

Example: FR DLCI=72

Dependencies: This parameter is not applicable if Frame Relay encapsulation is in use.

Location: Ethernet > Connections > Session Options

See Also: FR Direct

FR Link Down

Description: Specifies whether a trap is sent whenever a DLCI is brought down.

Usage: Specify Yes or No. The default is Yes.

- Yes specifies that a trap is sent whenever a DLCI is brought down.
- No specifies that a trap is not sent whenever a DLCI is brought down.

Example: `FR Link Doyennes`

Location: Ethernet > SNMP Traps > Enable Traps

See Also: FR Link Up, Link Down, Link Up

FR Link Up

Description: Specifies whether a trap is sent whenever a DLCI is brought up.

Usage: You can specify Yes or No. The default is Yes.

- Yes specifies that a trap is sent whenever a DLCI is brought up. The default is Yes.
- No specifies that a trap is not sent whenever a DLCI is brought up.

Example: `FR Link Yuppies`

Location: Ethernet > SNMP Traps > Enable Traps

See Also: FR Link Down, Link Down, Link Up

Front End

Description: Specifies the front-end type of the T1 or E1 transceiver.

Usage: For a T1 line, specify one of the following values:

- CSU specifies a Channel Service Unit, a device that ensures that only clean signals go out on the line.
- DSX specifies Digital Signal Cross-Connect interfaces for connecting DS1 and DS3 signals.

For an E1 line, specify one of the following values:

- Long-Haul (120-ohm termination only)
- Short-Haul

Example: `Front Nudists`

Location: Net/8T1 > Line Config > Line *N*, Net/8E1 > Line Config > Line *N*

See Also: Bulldog, Clock Source, Encoding, Framing Mode, Length

FR Prof

Description: Specifies the name of the Frame Relay profile to use for forwarding this link on the Frame Relay network.

Usage: Specify the name of a configured Frame Relay profile. This is the string assigned in the Name parameter of the Frame Relay profile, specified respecting case sensitivity.

Example: `FR Prof=pacbell`

Location: Ethernet > Connections > Encaps Options, Ethernet > Connections > Session Options

See Also: FR Type, DLCI

FR Type

Description: Specifies the type of interface between the DSL Terminator unit and a Frame Relay switch or customer premises equipment (CPE) on the Frame Relay network.

Note: For NNI or UNI-DTE connections, the DSL Terminator unit is able to query the device at the other end of the link about the status of the DLCIs in the connection. If any of the DLCIs become unusable and the DLCIs Connection profile has a specified Backup connection, the DSL Terminator unit dials the Connection profile specified in the Backup parameter in the Session Options submenu.

Usage: Specify one of the following values:

- NNI (Network-to-Network Interface) An NNI interface connection allows the DSL Terminator unit to appear as a Frame Relay network interface based on the NNI specifications. It performs both DTE and DCE link management, and allows two separate Frame Relay networks to connect via a common protocol.
- UNI-DCE (User to network interface—Data Communications Equipment) UNI is the interface between an end-user and a network end point (a router or a switch) on the Frame Relay network. In a UNI-DCE connection, the DSL Terminator unit operates as a Frame Relay router communicating with a Data Terminal Equipment (DTE) device. To the DTE devices, it appears as a Frame Relay network end point.
- UNI-DTE (User-to-Network Interface—Data Terminal Equipment) In a UNI-DTE connection, the DSL Terminator unit is configured as a UNI-DTE communicating with a Frame Relay switch. It acts as a Frame Relay *feeder* and performs the DTE functions specified for link management.

Example: `FR Type=NNI`

Location: Ethernet > Frame Relay

See Also: Circuit, DLCI, FR Prof, LinkUp

FT1 Caller

Description: Specifies whether the DSL Terminator unit initiates a Nailed/MPP call, or whether it waits for the remote end to initiate this type of call. If the remote end has FT1 Caller set to No, set it to Yes on the local DSL Terminator unit; by the same token, if the remote end has FT1 Caller set to Yes, set it to No on the local DSL Terminator unit.

Usage: Specify Yes or No. No is the default.

- Yes means the unit can initiate Nailed/MPP calls using this profile.
- No means the unit cannot initiate these calls.

Example: `FT1 Caller=Yes`

Dependencies: This parameter applies only when the call type is Nailed/MPP.

Location: Ethernet > Connections > Telco Options

See Also: Call Type

G

Gateway

Description: Specifies the IP address of the next-hop router that a packet must go through to reach the route's destination address. A next-hop router is either directly connected (on Ethernet) or is one hop away on a WAN link.

Usage: Specify the IP address of the next-hop router.

Example: `Gateway=10.3.3.100`

Dependencies: This parameter does not apply if the DSL Terminator unit does not support IP routing.

Location: Ethernet > Static Rtes

See Also: Dest

GRE MTU

Description: Specifies a lower Maximum Transmission Unit (MTU) value than the actual path MTU of the link between an Ascend Tunnel Management Protocol (ATMP) Foreign Agent and Home Agent. The actual path MTU is determined by the type of connection.

Mobile Clients use standard MTU discovery mechanisms to determine the path MTU, and then fragment packets at the appropriate size. However, to transmit packets through an ATMP tunnel, the DSL Terminator unit adds an 8-byte GRE header and a 20-byte IP header to the frames it receives. This action can make the packet size larger than the MTU of the tunneled link, in which case the DSL Terminator unit must either fragment the packet after encapsulating it, or reject the packet.

Usage: To avoid fragmenting packets after encapsulating them, set GRE MTU to a value that is 28 bytes less than the path MTU. If GRE MTU is set to zero (the default), the DSL Terminator unit might have to fragment encapsulated packets before transmission. The other ATMP agent must then reassemble the packets. If the GRE MTU value is greater than zero, the DSL Terminator unit reports that value to the client software as the path MTU, causing the client to send packets at the specified size. Setting GRE MTU to a nonzero value pushes the task of fragmentation and reassembly out to the connection endpoints, lowering the overhead on the ATMP agents.

Example: `GRE MTU=1000`

Location: Ethernet > Mode Config > ATMP Options

See Also: Force Fragmentation

Group

Description: Assigns a group of nailed channels to a connection. Nailed channels are used for permanent connections, which are typically leased. It is important to keep those channels dedicated to the connection. Do not assign the same group number to more than one profile of any type.

Usage: Specify the group number assigned to nailed channels in a Line profile.

Example: `Group=6`

Location: Ethernet > Connections > Telco Options

See Also: Call Type

GRP Leave Delay

Description: Specifies the amount of seconds the DSL Terminator unit waits before forwarding any IGMP, version 2, `leave group` message from any multicast client. If you specify a value other than 0 and the DSL Terminator unit receives a `leave group` message, the unit sends an IGMP query to the WAN interface from which it received the `leave group` message. If the unit does not receive a response from an active multicast client from the same group from the WAN interface, it sends a `leave group` message when the time specified in the GRP Leave Delay parameter has expired.

Usage: Specify a number of seconds from 0 to 120. The default is 0 (zero), which specifies that the DSL Terminator unit forwards any `leave group` message immediately. If users might establish multiple multicast sessions for identical groups, you should set GRP Leave Delay to a value between 10 and 20 seconds.

Example: `GRP Leave Delay=15`

Dependencies: `GRP Leave Delay` applies only if `Forwarding` is set to Yes and `Multicast Client` is set to Yes.

Location: Ethernet > Mod Config > Multicast

See Also: Forwarding, Multicast Client

H

HeartBeat Addr

Description: Specifies a multicast address. The DSL Terminator unit listens for packets to and from this group to perform the heartbeat-monitoring feature. When it is running as a multicast forwarder, the unit DSL Terminator continually receives multicast traffic. The heartbeat-monitoring feature enables the administrator to monitor possible connectivity problems by continuously polling for this traffic and generating an SNMP alarm trap if there is a traffic breakdown.

Note: Heartbeat monitoring is optional. It is not required for multicast forwarding.

Usage: Specify a multicast address to use for heartbeat monitoring.

Example: `HeartBeat Addr=224.1.1.1`

Dependencies: To set up heartbeat monitoring, you must configure several parameters that define what packets are monitored, how often and for how long to poll for multicast packets, and the threshold for generating an alarm. These parameters do not apply if multicast forwarding is not in use.

Location: Ethernet > Mod Config > Multicast

See Also: Alarm Threshold ,HeartBeat Slot Time, HeartBeat Slot Count, HeartBeat Udp Port, Source Addr, Source Mask

See Also:

HeartBeat Slot Count

Description: Specifies how many times to poll for multicast traffic before comparing the number of heartbeat packets received to the Alarm Threshold. The DSL Terminator unit polls for multicast traffic the specified number of times, waits for the interval specified in the HeartBeat Slot Time parameter, and then polls again.

Note: Heartbeat monitoring is optional. It is not required for multicast forwarding.

Usage: Specify a number of seconds.

Example: `HeartBeat Slot Count=10`

Dependencies: To set up heartbeat monitoring, you must configure several parameters that define what packets will be monitored, how often and for how long to poll for multicast packets, and the threshold for generating an alarm. These parameters do not apply if multicast forwarding is not in use.

Location: Ethernet > Mod Config > Multicast

See Also: Alarm Threshold, HeartBeat Addr, HeartBeat Slot Time, Heartbeat Udp Port, Source Addr, Source Mask

HeartBeat Slot Time

Description: Specifies how often (in seconds) the DSL Terminator unit should poll for multicast traffic. The unit polls for multicast traffic, waits for the specified interval, and then polls again.

Note: Heartbeat monitoring is optional. It is not required for multicast forwarding.

Usage: Specify a number of seconds.

Example: `HeartBeat Slot Time=10`

Dependencies: To set up heartbeat monitoring, you must configure several parameters that define what packets will be monitored, how often and for how long to poll for multicast packets, and the threshold for generating an alarm. These parameters do not apply if multicast forwarding is not in use.

Location: Ethernet > Mod Config > Multicast

See Also: Alarm Threshold, HeartBeat Addr, HeartBeat Slot Count, Heartbeat Udp Port, Source Addr, Source Mask

HeartBeat Udp Port

Description: Specifies a UDP port number. The DSL Terminator unit listens only to packets received on that port to perform the heartbeat-monitoring feature. When it is running as a multicast forwarder, the unit continuously receives multicast traffic. The heartbeat-monitoring feature enables the administrator to monitor possible connectivity problems by continuously polling for this traffic and generating an SNMP alarm trap if there is a traffic breakdown.

Note: Heartbeat monitoring is optional. It is not required for multicast forwarding.

Usage: Specify a UDP port to use for heartbeat monitoring.

Example: `HeartBeat Udp Port=16387`

Dependencies: To set up heartbeat monitoring, you must configure several parameters that define what packets will be monitored, how often and for how long to poll for multicast packets, and the threshold for generating an alarm. These parameters do not apply if multicast forwarding is not in use.

Location: Ethernet > Mod Config > Multicast

See Also: HeartBeat Addr, HeartBeat Slot Count, HeartBeat Slot Time, Source Addr, Source MaskAlarm Threshold

High BER

Description: 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.

Usage: Specify one of the following values:

- 10**-3 (the default)

- 10**-4
- 10**-5

Location: System > Sys Config

See Also: High BER Alarm

High BER Alarm

Description: Description: Specifies whether the back panel alarm relay closes when the bit-error rate exceeds the value specified by the High BER parameter. The MAX has an alarm relay whose contacts remain open on the back panel's alarm relay terminal block during normal operation. If you enable them, the alarm relay contacts close during loss of power, hardware failure, or a system reset. The High BER Alarm parameter specifies whether the contacts also close when the bit-error rate exceeds the High BER parameter value.

Usage: Specify Yes or No. No is the default.

- Yes causes the MAX to close the back panel alarm relay when the bit-error rate exceeds the High BER value.
- No causes the MAX to log the event but not close the alarm relay.

Example: `High BER Alarm=Yes`

Location: System > Sys Config

See Also: High BER

Host #*N*

Description: Specifies the IP address of a call-log host.

The DSL Terminator unit first tries to connect to Host #1. If it receives no response, it tries to connect to Host #2. If it still receives no response, it tries Host #3. If the DSL Terminator unit connects to a host other than Host #1, it continues to use that host until it fails to service requests, even if the first host has come back online.

Usage: Specify an IP address in dotted decimal notation. The default is 0.0.0.0.

Example: `Host #1=224.1.1.1`

Dependencies: If Call Log=No, Host #*N* does not apply.

Location: Ethernet > Mod Config > Call Logging

See Also: Acct-ID Base, Allow Stop Only, Call Log, Call Log Timeout, Dst Port, Key, Max Retry, Reset Timeout

I

ICMP Redirects

Description: Specifies whether the DSL Terminator unit accepts or ignores Internet ICMP Redirect packets. ICMP was designed to dynamically find the most efficient IP route to a destination. ICMP redirect packets are one of the oldest route discovery methods on the Internet and one of the least secure because it is possible to counterfeit ICMP redirects and change the way a device routes packets.

Usage: Specify one of the following values:

- Accept (to process ICMP redirects). This is the default.
- Ignore (to drop ICMP redirects)

Example: `ICMP Redirects=Ignore`

Location: Ethernet > Mod Config

Idle

Description: Specifies the number of seconds the DSL Terminator unit waits before clearing a call when a session is inactive.

Usage: Specify the number of seconds a session can remain idle without being brought down. If you specify 0 (zero), the DSL Terminator unit does not enforce a limit; an idle connection stays open indefinitely. The default setting is 120 seconds.

Example: `Idle=100`

Location: Ethernet > Answer > Session Options, Ethernet > Connections > Session Options

See Also: Call Type, Profile Reqd

Idle Limit

Description: Specifies the number of minutes that the Home Agent maintains an idle tunnel before disconnecting it.

Usage: Specify a number from 0 to 65535. The default is 0 (zero) minutes. Setting a value of 0 (zero) disables the idle timer, so that an idle tunnel is maintained indefinitely.

Example: `Idle Limit=50000`

Location: Ethernet > Mod Config > ATMP Options

See Also: ATMP Mode, ATMP Gateway

Idle Logout

Description: Specifies the number of minutes an administrative login can remain inactive before the DSL Terminator unit logs out and hangs up.

Usage: Specify a number between 0 and 60. The default setting is 0; this setting disables automatic logout.

Example: `Idle Logout=50`

Location: System > Sys Config

Idle Pct

Description: Specifies a percentage of bandwidth utilization below which the DSL Terminator unit clears an MP+ call. Bandwidth utilization must fall below this percentage *on both sides of the connection* before the DSL Terminator unit clears the call.

If the device at the remote end of the link specifies an Idle Pct setting lower than the value you specified at the local end, the DSL Terminator unit does not clear the call until bandwidth utilization falls below the lower percentage. If either end of a connection sets this parameter to 0 (zero), the DSL Terminator unit ignores the parameter on both sides.

Note: When bandwidth utilization falls below the Idle Pct setting on both sides of the connection, the call disconnects regardless of whether the time specified by the Idle parameter has expired.

Usage: Specify a number between 0 and 99. The default value is 0; a 0 setting causes the DSL Terminator unit to ignore bandwidth utilization when determining whether to clear a call.

Example: `Idle Pct=50`

Dependencies: This parameter applies only to MP+ calls.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options

See Also: Call Filter, Encaps, Idle

IF Adrs

Description: Specifies a numbered interface IP address for the DSL Terminator unit. Interface-based routing allows the unit to operate more nearly the way a multihomed Internet host behaves. In addition to the systemwide IP configuration, the DSL Terminator unit and the far end of the link have link-specific IP addresses. The DSL Terminator unit address for this connection is specified in the IF Adrs parameter. The far end numbered interface address is specified in the WAN Alias parameter.

Usage: Specify the IP address of the numbered interface.

Example: `IF Adr=10.207.23.7/24`

Dependencies: This parameter does not apply if the DSL Terminator unit does not route IP.

Location: Ethernet > Connections > IP options

See Also: WAN Alias, Route IP

Ignore Def Rt

Description: Specifies whether the DSL Terminator unit ignores the default route when updating its routing table via RIP updates. The default route specifies a static route to another IP router, which is often a local router such as a Cisco router or another kind of LAN router. When the DSL Terminator unit is configured to ignore the default route, RIP updates will not modify the default route in the routing table.

Usage: Specify Yes or No.

- Yes means the DSL Terminator unit ignore advertised default routes. This is recommended.
- No means the DSL Terminator unit may modify its default route based on RIP updates. No is the default.

Example: `Ignore Def Rt=Yes`

Dependencies: This parameter is not applicable if the DSL Terminator unit does not route IP.

Location: Ethernet > Mod Config > Ether Options

Inc Ch Count

Description: Specifies the number of channels the DSL Terminator adds as a bundle when bandwidth changes either manually or automatically during a call. If the call's data service is 384K/H0 or 384KR, the value you specify should be divisible by 6, because 384 kbps is 6x64 kbps. In this case, specify a value of 6, 12, 18, 24, or 30. If the call's data service is MultiRate or GloBanD, and the service you select is a multiple of 64 kbps, specify a value that is a multiple of 6. MP+ calls cannot exceed 32 channels. The sum of Base Ch Count and Inc Ch Count cannot exceed the maximum number of channels available.

Usage: Usage: Specify a number of channels. The default is 1.

Example: `Inc Ch Count=3`

Dependencies: This parameter does not apply if the call type is Nailed. In a Call profile, this parameter applies only if the call type is AIM, FT1-AIM, FT1-B&O, or BONDING and the Call Mgm parameter is set to Manual, Dynamic, or Mode 2.

Location: Ethernet > Connections >

Inverse ARP

Description: Specifies whether Inverse ARP is enabled for this ATM connection.

Usage: Specify one of the following values.

- Yes enables Inverse ARP for the connection.
- No (the default) disables Inverse ARP for the connection.

Example: `Inverse ARP=Yes`

Dependencies: Consider the following:

- IP routing must be enabled in the Connection profile for Inverse ARP to apply.

- The Connection profile must specify ATM encapsulation.

Location: Ethernet > Connections > Connection profile > Encaps Options

IP Adrs

Description: Specifies the LAN interface IP address.

Usage: Specify the IP address of the DSL Terminator unit on the local IP network or subnet.

Example: `IP Adrs=10.2.1.1/24`

Dependencies: This parameter does not apply if the DSL Terminator unit does not route IP.

Location: Ethernet > Mod Config > Ether Options

See Also: Encaps, Route IP

IP Direct

Description: Specifies the IP address of a local host that all inbound IP packets on this link will be directed. When you specify an address for this parameter, the DSL Terminator unit bypasses all internal routing and bridging tables and sends each packet received from the remote end of the connection to the specified address. This does not affect outbound traffic. Note that the IP direct host must be on the same local network as the DSL Terminator unit.

Usage: Specify an IP address. The default is 0.0.0.0. If you accept the default, the DSL Terminator unit does not redirect traffic coming from the remote end specified by the Connection profile.

Example: `IP Direct=10.2.3.4/24`

Location: Ethernet > Connections > Session Options

See Also: Bridge, Encaps, FR Direct, RIP, Route IP

K

Keep User Name

Description: Specifies User-Name attribute handling in RADIUS.

Usage: Specify one of the following settings:

- Change Name (the default) indicates that the name provided by the server is used for the status display and for RADIUS accounting purposes.
- Keep Name specifies that the DSL Terminator unit does not use the User-Name returned by the server. If a name has been specified (that is, if CLID or DNIS authentication is not used), the system uses that name. Otherwise, it uses the name sent to the server for authentication.
- Keep Realm specifies that if the username sent to the server for authentication is in a realm (for example, if it contains one of the characters `@\/%`), the system behaves as if Keep User Name were set to Keep Name. Otherwise, the system behaves as if Change Name were specified.

Example: `Keep User Name=Keep Name`

Dependencies: A user authenticated by CLID or DNIS appears to have the CLID or DNIS number as username. If this condition is a problem, set Keep User Name to Keep Realm Name.

Location: Ethernet > Mod Config > Auth

Key

Description: Specifies a shared secret that enables the call-logging host to recognize data from the DSL Terminator unit. A shared secret acts as a password between the DSL Terminator unit and the call-log host.

Usage: Specify the text of the shared secret. The value you specify must match the value configured on the call-logging host. The default is null.

Example: `Key=Oursecret`

Dependencies: If Call Log=No, Key does not apply.

Location: Ethernet > Mod Config > Call Logging

Acct-ID Base, Allow Stop Only, Call Log, Call Log Timeout, Dst Port, Host # N, Max Retry, Reset Timeout

KeyID

Description: Specifies an authentication key (a password) used to allow OSPF routing. KeyID is a number from 0 to 255 inserted into the OSPF packet header. OSPF routers use KeyId to allow or exclude packets from an area. The default value is `0`.

Usage: Specify a number from 0 to 255.

Example: `KeyID=125`

Dependencies: KeyID does not apply unless you set AuthType to MD5.

Location: Ethernet > Connections > OSPF Options, Ethernet > Mod Config > OSPF Options

See Also: AuthType, MD5 Key

L

L2TP Auth Enabled

Description: Enables or disables L2TP tunnel authentication.

Usage: Specify Yes or No. If N/A is displayed, change L2TP Mode.

- Yes specifies that the DSL Terminator unit authenticates the L2TP Network Server (LNS) with a shared secret before passing calls to the system.
- No specifies that the DSL Terminator unit does not authenticate the LNS. The default is No.

Example: `L2TP Auth Enabled=Yes`

Dependencies: You must either enable tunnel authentication for both the LAC and LNS or enable it for neither. You configure a tunnel password in a Name-Password profile. If you are using RADIUS with L2TP, the RADIUS server must be able to encrypt the Tunnel-Password attribute. Not all RADIUS servers can do so. NavisRadius, Ascend RADIUS, and Ascend Access Control can encrypt the Tunnel-Password value.

Location: Ethernet > Mod Config > L2 Tunneling Options

See Also: L2TP Mode, L2TP RX Window

L2TP Mode

Description: Specifies the systemwide type of L2TP functionality the DSL Terminator unit supports.

Usage: Specify one of the following values:

- LAC specifies that the DSL Terminator unit can function as an LAC only.
- LNS specifies that the DSL Terminator unit can function as an LNS only.
- Both specifies that the DSL Terminator unit can function as either an LAC or an LNS.
- None disables L2TP functionality on the DSL Terminator unit. None is the default.

Example: `L2TP Enable=Both`

Location: Ethernet > Mod Config > L2 Tunneling Options

See Also: L2TP Auth, L2TP RX Window, Line *n* tunnel type, Route *n* line

L2TP RX Window

Description: Specifies the advertised L2TP receive window size for data channels.

Usage: Specify an integer. The default is 0 (zero), which indicates that the DSL Terminator unit will ask for no flow control for inbound L2TP payloads.

Example: `RX Window=15`

Location: Ethernet > Mod Config > L2 Tunneling Options

See Also: L2TP Auth, L2TP Mode, Line *n* tunnel type, Route *n* line

LAN Adrs

Description: Specifies the IP address of remote-end host or router.

Usage: Specify the IP address of the remote device.

Example: `LAN Adrs=200.207.23.101/24`

Dependencies: This parameter does not apply if the DSL Terminator unit does not support IP routing. No two calling Connection profiles should have the same LAN Adrs.

Location: Ethernet > Connections > IP Options

See Also: Encaps, IP Adrs, Route IP, Station

Last DS0 Channel

Description: Specifies the last DS0 for the nailed T1 or E1 line. Get this information from your WAN service provider.

Usage: Specify the last DS0. You can specify a number between 1 and 24 (for T1) or 1 and 32 (for E1).

Example: `Last DS0 Channel=24`

Dependencies: Last DS0 Channel must be set to a value greater than the First DS0 Channel value.

Location: Net/8T1 > Line Config > Line *N*, Net/8E1 > Line Config > Line *N*

See Also: First DS0 Channel

Length

Description: In a T1 line profile, specifies the cable length of the line from the Channel Service Unit (CSU) or other network interface unit to the DSL Terminator unit. The setting you indicate should reflect the longest line length you expect to encounter in your installation.

In a Firewall profile, it specifies the length of the firewall uploaded to the DSL Terminator unit from Secure Access Manager (SAM). In Firewall profiles, the parameter is read-only.

In a filter of type Generic, specifies the number of bytes to test in a frame, starting at the specified Offset. The DSL Terminator unit compares the contents of those bytes to the value specified in the filter's Value parameter.

Usage: In a T1 line profile, specify one of the following values in feet:

- 1–133 (the default)
- 134–266
- 267–399
- 400–599

In a Filter profile, specify a number between 0 and 8 that defines the number of bytes to use for comparison. The default zero means no bytes are compared.

Example: With this specification:

```
Filters
   Name=filter-name
   Input filters...
      In filter 01
         Generic...
            Forward=No
            Offset=2
            Length=8
            Mask=0F FF FF FF 00 00 00 F0
            Value=07 FE 45 70 00 00 00 90
            Compare=Equals
            More=No
```

and the following packet contents:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

The filter applies the mask only to the eight bytes following the two-byte offset.

Dependencies: In a T1 line profile, Length applies only when Front End=DSX.

Location: Ethernet > Filters > Input filters > In filter *N* > Generic, Ethernet > Filters > Output filters > Out filter *N* > Generic, Ethernet > Firewalls, Net/8T1 > Line Config > Line *N*

See Also: Buildout, Clock Source, Framing Mode, Front End, Offset, Mask, Value

Line Rate

Description: Specifies the symmetrical data rate.

Usage: Specify one of the following values:

144000
272000
400000
528000
784000 (the default)
1168000
1552000

Example: `Line Rate=160000`

Location: Net/SDSL-8 > Line Config > Line *N*, Net/SDSL-16 > Line Config > Line *N*

See Also: Activation, Enabled, Nailed-Group, Rate Mode, TrnkGrp, Unit Type

Line *N* Tunnel Type

Description: Indicates whether the DSL Terminator unit should tunnel all calls received on the specified WAN line.

Usage: Specify one of the following values:

- L2TP directs the DSL Terminator unit to create L2TP tunnels for all calls received on the specified line.
- PPTP directs the DSL Terminator unit to create PPTP tunnels for all calls received on the specified line.
- None directs the DSL Terminator unit not to create tunnels on a per-line basis.

  None is the default.

Example: `Line 1 Tunnel Type=None`

Dependencies: Line n tunnel type applies only if you set L2TP Mode to LAC or Both.

Location: Ethernet > Mod Config > L2 Tunneling Options

See Also: L2TP Mode, Route *N* Line

Line Type

Description: Specifies whether the serial WAN is a physical DCE or DTE.

Usage: Specify DCE or DTE.

Note: The parameter FR Type in Ethernet > Frame Relay > *any profile* has values of DCE, DTE or NMI. This is unrelated to the physical mode of the interface. It is possible to be a DCE in this profile but be a physical DTE and vice versa.

When you connect two serial devices together one should be a DCE and one a DTE. Usually your switch is the DCE and the MAX is the DTE. However the MAX 3000 can also act as a DCE to plug another unit into. DCE and DTE have different pin outs and it is the DCE which supplies the clock.

Example: `Line Type=DTE`

Dependencies: When the Line Type parameter is set to DTE, the Line Speed parameter will be N/A.

Location: Serial WAN > Mod Config

Link Comp

Description: Specifies the link compression method for a PPP, MP, and MP+ call. Both sides of the connection must set the same type of link compression or it will not be used.

Usage: Specify one of the following values:

- None (the default in the Answer profile and Connection profile).
- Stac (Use a modified version of draft 0 of the CCP protocol).
- Stac-9 (Use draft 9 of the Stac LZS Compression protocol).
- MS-Stac. Use Microsoft/Stac compression (the same method as Windows95). If the caller does not acknowledge Microsoft/Stac compression, the DSL Terminator unit attempts to use standard Stac compression; if that does not work, it uses no compression.

Example: `Link Comp=Stac`

Dependencies: This parameter applies only to PPP and its multilink variants. Both sides of the link must support the same kind of compression or it is not used.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options

See Also: VJ Comp

Link Down

Description: Specifies whether the system generates a trap when a failure occurs in a communication link between the unit and the SNMP manager.

Usage: Specify Yes or No.

- Yes specifies that the system generates a trap when a failure occurs in a communication link between the unit and the SNMP manager. The default is Yes.
- No specifies that the system does not generate a trap when a failure occurs in a communication link between the unit and the SNMP manager.

Example: `Link Down=No`

Location: Ethernet > SNMP Traps > Enable Traps

See Also: Link Up

Link Mgmt

Description: Specifies the link management protocol to use between the DSL Terminator unit and the Frame Relay switch. The Frame Relay administrator or service provider can tell you which value to use.

Usage: Specify one of the following values:

- None specifies no link management. The DSL Terminator unit assumes that the physical link is up and that all logical links (as defined by the DLCI and FR DLCI parameters) are active on the physical link. None is the default.
- T1.617D specifies the link management protocol defined in ANSI T1.617 Annex D.
- Q.933A the link management protocol defined Q.933 Annex A.

Example: `Link Mgmt=Q.9993A`

Location: Ethernet > Frame Relay

See Also: DLCI, FR DLCI

Link Status DLCI

Description: Specifies the DLCI to use for link management on the Frame Relay datalink.

Usage: Specify DLCI0 (the default) or DLCI1023.

Example: `Link Status DLCI=`DLCI1023

Location: Ethernet > Frame Relay

See Also: Link Mgmt

Link Up

Description: Specifies whether the system generates a trap when the communication link between the unit and the SNMP manager comes back up.

Usage: Specify Yes or No.

- Yes specifies that the system generates a trap when the communication link between the unit and the SNMP manager comes back up. The default is Yes.
- No specifies that the system does not generate a trap when the communication link between the unit and the SNMP manager comes back up.

Example: `Link Up=No`

Location: Ethernet > SNMP Traps > Enable Traps

See Also: Link Down

Local Profiles First

Description: Specifies whether the DSL Terminator unit should attempt local authentication before remote (external) authentication. By default, the DSL Terminator unit first attempts to authenticate the connection using local profiles. If that fails, the DSL Terminator unit tries to authenticate the connection using an external authentication server.

If this parameter set to No, the DSL Terminator unit first tries to authenticate the connection using a remote authentication server. If that fails, the DSL Terminator unit attempts to authenticate the connection using local profiles. In this case, some dynamic password challenges behave differently than when authentication is local. (PAP and CHAP work the same either way.)

- PAP-TOKEN. Authentication will not produce a challenge if there is a local profile. This defeats the security of using PAP-TOKEN.
- PAP-TOKEN-CHAP. Brings up one channel, but all other channels fail.
- CACHE-TOKEN. If the far end of the connection has ever authenticated using a challenge, CACHE-TOKEN will not work with local profiles. If the far end has not even been authenticated, there is no problem with the local profiles.

Note: Because the remote authentication is tried first if this parameter set to No, the DSL Terminator unit waits for the remote authentication to time out before attempting to authenticate locally. This timeout may take longer than the timeout specified for the connection and could cause all connection attempts to fail. To prevent Connection failure, set the authentication timeout value low enough not to cause the line to be dropped, but still high enough to permit the unit to respond if it is able to. The recommended time is 3 seconds.

Usage: Specify Yes or No.

- Yes retains the default authentication order. Yes is the default.
- No reverses the default and attempts remote authentication first.

Example: `Local Profiles First=Yes`

Dependencies: This parameter is not applicable if Auth is set to None. See the Note above for related dependencies.

Location: Ethernet > Mod Config > Auth

See Also: Auth Timeout

Location

Description: This is an SNMP-readable parameter that specifies the physical location of the DSL Terminator unit. It does not affect the unit's operations.

Usage: Specify a description of the DSL Terminator unit's location. You can enter up to 80 characters.

Example: `Location=Ascend_Alameda`

Location: System > Sys Config

See Also: Contact

Log Call Info

Description: Specifies whether, at the time an authenticated call ends, the DSL Terminator unit reports to Syslog the following information about the call:

- Station name
- Calling phone number
- Called phone number
- Encapsulation protocol
- Data rate (in bits per second)
- Progress code or disconnect reason
- Number of seconds before authentication
- Number of bytes or packets received during authentication
- Number of bytes or packets sent during authentication
- Length of session (in seconds)
- Number of bytes or packets received during the session
- Number of bytes or packets sent during the session

A one-line Syslog message contains information about the terminated call. If some of the information is not available, that field is displayed as either a question-mark (for strings) or a zero (for numerals).

Usage: To specify that the DSL Terminator unit reports the information to Syslog, specify EndOfCall. To specify that the unit does not report the information, specify None (the default).

Example: `Log Call info=EndOfCall`

Dependencies: Consider the following:

- Use Log Call Info only for diagnosing session problems. The reports to Syslog rely on the UDP protocol, which does not guarantee delivery. Therefore, you should not use Log Call Info for billing purposes.
- Log Call Info applies only if Syslog=Yes.

Location: Ethernet > Mod Config >Log

See Also: Log Facility, Log Host

Log Call Progress

Description: Specifies whether the DSL Terminator unit receives incoming call-progress Syslog messages. Log Call Progress controls the reception and output of the following messages:

- Incoming call
- Call answered
- Assigned to port
- Call connected
- LAN session up
- Call terminated
- LAN session down
- Call cleared

Usage: Specify Yes or No.

- Yes specifies that the DSL Terminator unit receives incoming call-progress Syslog messages.
- No specifies that the DSL Terminator unit does not receive incoming call-progress Syslog messages. The default is No.

Example: `Log Call Progress=Yes`

Location: Ethernet > Mod Config > Log

See Also: Log Software Version

Log Facility

Description: Specifies how the Syslog host sorts system logs. The Syslog host is the station to which the DSL Terminator unit sends system logs.

All system logs using the same setting are grouped together in the host's file system. That is, all system logs using the Local0 facility are grouped together, all system logs using the Local1 facility are grouped together, and so on.

Usage: Specify one of the following values:

- Local0 (the default)
- Local1
- Local2

- Local3
- Local4
- Local5
- Local6
- Local7

Example: `Log Facility=Local3`

Dependencies: This parameter applies only when Syslog=Yes.

Location: Ethernet > Mod Config > Log

See Also: Log Host, Syslog

Log Host

Description: Specifies the IP address of the Syslog host—a UNIX station to which the DSL Terminator unit sends system logs.

Usage: Specify the IP address of Syslog host. The default value is 0.0.0.0.

Example: `Log Host=10.207.23.1`

Dependencies: This parameter applies only when Syslog=Yes.

Location: Ethernet > Mod Config > Log

See Also: Log Facility, Log Port, Syslog

Log Port

Description: Specifies the destination port of the Syslog host.

Usage: Specify a port number. The default is 514.

Example: `Log Port=1260`

Dependencies: Log Port applies only if Syslog=Yes.

Location: Ethernet > Mod Config > Log

See Also: Log Host, Syslog

Log Software Version

Description: Specifies whether the DSL Terminator unit reports the current software version every hour.

Usage: Specify Yes or No.

- Yes specifies that the unit reports the current software version every hour.
- No specifies that the unit does not report the current software version every hour. The default is No.

Example: `Log Software Version=Yes`

Location: Ethernet > Mod Config > Log

See Also: Log Call Progress

Long Cable

Description: Specifies whether the DS3 cable length is more than 255 ft.

Usage: Specify Yes or No. The default is No.

Example: `Long Cable=Yes`

Location: Net/ATM-DS3 > Line Config > Line *N*

See Also: Nailed-Group

LQM

Description: Specifies whether the DSL Terminator unit requests Link Quality Monitoring (LQM) when answering a PPP call. LQM counts the number of packets sent across the link and periodically asks the remote end how many packets it has received. Discrepancies are evidence of packet loss and indicate link quality problems.

Both sides of the link negotiate the interval between periodic link quality reports; however, the interval must fall between the minimum interval (LQM Min) and the maximum interval (LQM Max).

Usage: Specify Yes or No.

- Yes enables link quality monitoring for PPP connections.
- No turns off LQM. No is the default.

Example: `LQM=Yes`

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options

Dependencies: This parameter applies only to PPP and its multilink variants.

See Also: Encaps, LQM Max, LQM Min

LQM Max

Description: Specifies the maximum duration between link quality reports for PPP connections, measured in 100ths of a second.

Usage: Specify a number between 0 and 600. The default is 600.

Example: `LQM Max=550`

Dependencies: This parameter applies only to PPP and its multilink variants. It is not applicable if LQM is set to No.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options

See Also: LQM, LQM Min

LQM Min

Description: Specifies the minimum duration between link quality reports for PPP connections, measured in 100ths of a second.

Usage: Specify a number between 0 and 600. The default is 600.

Example: `LQM Min=500`

Dependencies: This parameter applies only to PPP and its multilink variants. It is not applicable if LQM is set to No.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options

See Also: LQM, LQM Max

M

Mask

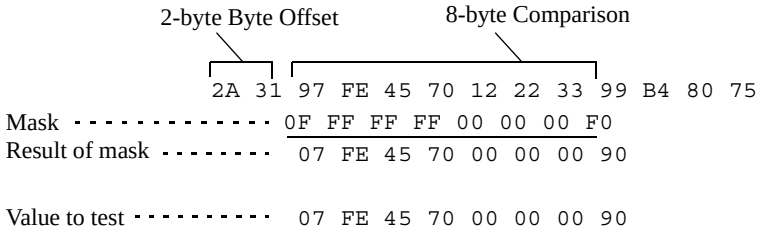
Description: In a filter of type Generic, specifies a 16-bit mask to apply to the Value parameter before comparing it to the packet contents at the specified offset. You can use it to fine-tune exactly which bits you want to compare. The DSL Terminator unit applies the mask to the specified value using a logical AND after the mask and value are both translated into binary format. The mask hides the bits that appear behind each binary 0 (zero) in the mask. A mask of all ones (FF FF FF FF FF FF FF FF) masks no bits, so the full Compare To value must match the packet contents. For example, with this filter specification:

```
Filters
   Name=filter-name
   Input filters...
      In filter 01
         Generic...
            Forward=No
            Offset=2
            Length=8
            Mask=0F FF FF FF 00 00 00 F0
            Value=07 FE 45 70 00 00 00 90
            Compare=Equals
            More=No
```

and the following packet contents:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

The mask is applied as shown below, resulting in a value that matches the Value.



The packet matches this filter. Because the Filter Action is “Discard”, the packet is dropped. The byte comparison works as follows:

- 2A and 31 are ignored due to the two-byte offset.
- 9 in the lower half of the third byte is ignored, because the mask has a 0 in its place. The 7 in the third byte matches the value parameter’s 7 in the upper half of that byte.
- F and E in the fourth byte match the value parameter for that byte.
- 4 and 5 in the fifth byte match the value parameter for that byte.
- 7 and 0 in the sixth byte match the value parameter for that byte.
- 12 and 22 and 33 in the seventh, eighth and ninth bytes are ignored because the mask has a 0 in those places.
- 9 in the tenth byte equals the matches the value parameter’s 9 in the lower half of that byte. The second 9 in the upper-half of the packet’s tenth byte is ignored because the mask has a 0 in its place.

Usage: Specify a 16-bit hexadecimal number. The default of all zeroes means the DSL Terminator unit uses the data in the packet as is for comparison purposes.

Example: `Mask=0FFFFFFF000000F0`

Location: Ethernet > Filters > Input filters > In filter *N* > Generic, Ethernet > Filters > Output filters > Out filter *N* > Generic

See Also: Length, Offset, Type, Value

Max ATMP Tunnels

Description: Defines the maximum number of active ATMP sessions for units configured as an ATMP Home agent. Changes take effect after the Connection Profile is saved, the connection is cleared, and then reestablished.

Usage: Press Enter to open the text field. Type the number of simultaneous ATMP sessions you want to allow through this ATMP Gateway. The default, 0 (zero), disables the parameter.

Example: `Max ATMP Tunnels=4`

Dependencies: Applies only to units configured as ATMP Home agents.

Location: Ethernet > Connections > Session Options menu.

See Also: ATMP Gateway, ATMP Mode

Max Burst Size

Description: Specifies the maximum number of ATM cells the virtual circuit using a Traffic Shaping profile can transmit to the network at the peak rate.

Usage: Specify a number between 2 and 255. The default is 2.

Example: `Max burst size=255`

Dependencies: The Traffic Shaper profile must be enabled for Max Burst Size to apply.

Location: Net/DS3-ATM > Line Config > *any line profile* > Traffic Shapers,
Net/OC3-SMF-ATM > Line Config > *any line profile* > Traffic Shapers,
Net/OC3-UTP-ATM > Line Config > *any line profile* > Traffic Shapers

See Also: Aggregate, Bit Rate, Enabled, Peak Rate, Priority, Traffic Shaper

Max Call Duration

Description: Specifies the maximum duration in minutes of an established session for an incoming call. The connection is checked once per minute, so the actual time of the call will be slightly longer (usually less than a minute longer) than the actual time you set.

Usage: Specify a value from 1-1440. The default is zero, which disables the timer.

Example: `Max Call Duration=0`

Location: Ethernet > Answer > Session Options, Ethernet > Connections > Session Options

Max Ch Count

Description: Specifies the maximum number of channels that can be allocated to a multilink connection. For optimum performance, both sides of the connection should specify the same maximum channel count.

Usage: Specify a number from 1 to 32. The default setting is 1.

Example: `Max Ch Count=5`

Dependencies: This parameter applies only to MP+ calls.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options

See Also: Base Ch Count, Encaps

Max-Dialout-Time

Description: Specifies the maximum number of seconds the system waits for a Call Setup Complete from the remote side when dialing out.

Usage: Specify an integer from 0 to 255. The default is 20 seconds. If set to Max-Dialout-Time to 0 (zero), the DSL Terminator uses its internal default of 20 seconds.

Example: In the following example, the dialout timer is set to 60 seconds:

```
admin> read system
SYSTEM read

admin> set max-dialout-time=60

admin> write
SYSTEM written
```

Dependencies: The Max-Dialout-Time setting does not influence the modem timeout to detect carrier. Modems have an internal timer that counts down from dialout to establishing carrier with the remote modem (including training), which for Rockwell modems has a default of 45 seconds.

Location: System

See Also: Idle Logout, Name, New NASPort ID, Parallel Dial, Perm Conn Update

Max DS0 Mins

Description: Specifies the maximum number of DS0 minutes a call can be online. In a Port profile, it applies to calls from the AIM port within the specified time period. In the System profile, it applies to calls from all ports on the DSL Terminator and to the Ethernet module.

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. When the usage exceeds the maximum specified by the Max DS0 Mins parameter, the DSL Terminator cannot place any more calls, and takes any existing calls offline.

The Max DS0 Mins parameter limits usage of switched channels, even if the DSL Terminator combines these channels with nailed-up ones; although the DSL Terminator disconnects the

switched channels when a call exceeds the value of Max DS0 Mins, the nailed-up channels remain connected.

Usage: Specify a number specifying the maximum number of DS0 minutes a call can be online before the DSL Terminator disconnects it. A value of 0 (zero) is not valid for this parameter.

- In a Port profile, specify a number from 1 to 2,142,720 (default 1).
- In a System profile, specify a number from 1 to 5,713,920 (default 1).

Example: `Max DS0 Mins=30`

Dependencies: This parameter does not apply if DS0 Min Rst=Off.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Port Config, System > Sys Config

See Also: DS0 Min Rst

Max Members

Description: Specifies the maximum number of datalinks allowed to join the MFR bundle. The default value is 1.

If set to a number higher than 1, administrators can add bandwidth to the bundle up to the specified number of datalinks. For example, if Max Members is set to 4 and the bundle has 2 datalinks, the administrator can add bandwidth dynamically by configuring another datalink profile with the bundle name.

Usage: Specify the maximum number of datalinks allowed to join the MFR value (default 1).

Example: `Max Members=4`

Location: Multi-Link FR

See Also: Bundle Name, MFR Type, Active, Min Bandwdth

Max Retry

Description: Specifies the maximum number of retries for call-logging packets. When the DSL Terminator unit is configured for call logging, it sends Start and Stop packets to the call-logging host in order to record connections. If the host does not acknowledge a packet within the number of seconds specified for Reset Timeout, the DSL Terminator unit tries again, resending the packet until the host responds, or dropping the packet if the queue of packets to be resent is full. You can limit the number of retries by setting a maximum.

Usage: To set the maximum number of retries for Start and Stop packets, set Max Retry to a value greater than 0 (zero). A value of 0 (the default) indicates an unlimited number of retries.

Example: `Max Retry=4`

Dependencies: The DSL Terminator unit always makes at least one attempt. For example, if you set the number of retries to 10, the unit makes 11 attempts: the original attempt plus 10 retries.

Location: Ethernet > Mod Config > Call Logging

See Also: Acct-ID Base, Allow Stop Only, Call Log, Call Log Timeout, Dst Port, Host # N, Key, Reset Timeout

Max. Time (min)

Description: Specifies the maximum connect time in minutes for the ARA dial-in. The DSL Terminator unit initiates an ARA disconnect when the specified time is up. The ARA link goes down cleanly, but remote users are not notified. Users will find out the ARA link is gone only when they try to access a device.

Note: The Max. Time parameter is not associated with the DSL Terminator unit unit's idle timer.

Usage: Specify a number between 1 and the maximum number of minutes the connection should stay up. The default setting is 0 (zero); this setting indicates an unlimited connection time.

Example: `Max Time=10`

Dependencies: This parameter applies only to ARA connections.

Location: Ethernet > Connections > Encaps Options

See Also: AppleTalk, ARA, Encaps, Passwor

Mbone Profile

Description: Specifies the name of a resident Connection profile to a multicast router on the WAN. The specified Connection profile must be resident. (It cannot be accessed via a RADIUS or TACACS server.) If the Mbone profile name is null and Multicast Forwarding is turned on, the DSL Terminator unit assumes that its Ethernet is the MBONE interface.

Usage: Specify the name of the Connection profile to a remote multicast router. If no name is specified, the DSL Terminator unit assumes the presence of a multicast router on its Ethernet interface.

Example: `Mbone profile=newyork`

Location: Ethernet > Mod Config > Multicast

Dependencies: This parameter does not apply if Multicast Forwarding is set to No.

See Also: Forwarding, Multicast Client

MD5 Key

Description: Specifies an authentication key (a password) used to allow OSPF routing. MD5 Key is a number from 0 to 255 inserted into the OSPF packet header. OSPF routers use MD5 Key to allow or exclude packets from an area. The default value is `0`. The key can contain as many as 16 characters.

Usage: Specify a key containing as many as 16 characters.

Example: `MD5 Key=234658902234658`

Dependencies: MD5 Key does not apply unless you set AuthType to MD5.

Location: Ethernet > Connections > OSPF Options, Ethernet > Mod Config > OSPF Options

AuthType, Key ID=

Membership Timeout

Description: Specifies the timeout (in seconds) for client responses to multicast polling messages. When you configure the DSL Terminator unit as a multicast forwarder, it forwards polling messages generated by the multicast router, and keeps track of active memberships from its client interfaces. If no client responds to the polling messages within the amount of time you specify for Membership Timeout, the DSL Terminator unit stops forwarding multicast traffic on that interface.

Usage: Specify an integer from 60 to 65535. The default is 360.

Example: `Membership Timeout=300`

Dependencies: If multicast forwarding is disabled, Membership Timeout does not apply.

Location: Ethernet > Mod Config > Multicast

See Also: Multicast Client, Multicast Rate Limit

Metric

Description: In a Connection or Route profile, specifies a RIP metric (a virtual hop count) associated with the IP route. In the Answer profile, it specifies the RIP metric of the IP link when the DSL Terminator unit validates an incoming call using RADIUS or TACACS and Use Answer as Default is enabled. The specified metric is a virtual hop count. The actual hop count includes the metric of each switched link in the route.

If two routes have the same preference value, the DSL Terminator unit chooses the route with the lowest metric. If you enable RIP (Routing Information Protocol) across the WAN in a Connection profile or an Answer profile, the hop count for the route can differ from the value of the Metric parameter in the Route profile because the DSL Terminator unit always uses the lower hop count.

Usage: Press Specify a number between 1 and 15. The default setting is 7. The higher the number you specify, the less likely that the DSL Terminator unit will bring the link or route online.

Example: `Metric=4`

Dependencies: This parameter does not apply if the DSL Terminator unit does not route IP. In the Answer profile, the Use Answer as Default parameter must also be enabled.

Location: Ethernet > Answer > IP Options, Ethernet > Connections > IP Options, Ethernet > Static Rtes

See Also: Private, RIP

MFR Type

Description: Specifies the type of MFR configuration. In this release, only the MFR-DTE type is supported.

Usage: Specify DTE-DTE.

Example: `MFR Type=DTE-DTE`

Location: Multi-Link FR

See Also: Bundle Name, Active, Max Members, Min Bandwdth

Min Bandwdth

Description: Specifies the minimum aggregated bandwidth before the bundle is considered inactive. In this release, you must leave the default zero value. Because of an unresolved problem in Frame Relay, if Min Bandwdth is set to any other value, data is not sent on the bundle.

Usage: Leave the default zero value.

Example: `Min Bandwdth=0`

Location: Multi-Link FR

See Also: Bundle Name, MFR Type, Active, Max Members

Min Ch Count

Description: Specifies the minimum number of channels that can be established for a multilink call. If this number of channels is not available, the multilink session is not established. For optimum performance, both sides of the multilink connection should set this parameter to the same value.

Usage: Specify a number between 1 and the maximum channel count. The default setting is 1.

Example: `Min Ch Count=1`

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options

See Also: Max Ch Count

More

Description: In a filter of type Generic, specifies whether the DSL Terminator unit includes the next filter condition before determining whether the frame matches the filter. If value is Yes, the current filter condition is linked to the one immediately following it, so the filter can examine multiple non-contiguous bytes within a packet. In effect, this parameter *marries* the current filter to the next one, so that the next filter is applied before the forwarding decision is made. The match occurs only if *both* non-contiguous bytes contain the specified values.

Usage: Specify Yes or No. No is the default.

- Yes links the current filter rule to the next one, so the next filter is applied before the forwarding decision is made.
- No does not link the current filter rule. The forwarding decision is made based solely on this rule.

Example: `More=Yes`

Dependencies: The next filter must be enabled.

Location: Ethernet > Filters > Input filters > In filter *N* > Generic, Ethernet > Filters > Output filters > Out filter *N* > Generic

See Also: Forward, Length, Offset, Type, Value, Valid

MP

Description: This enables incoming Multilink PPP (MP) connections, which use the encapsulation defined in RFC 1990. MP enables the DSL Terminator unit to interact with Multilink PPP-compliant equipment from other vendors to use multiple channels for a call. Both sides of the connection must support MP.

Usage: Specify Yes or No.

- Yes means the unit answers MP calls, provided that they meet all other criteria.Yes is the default.
- No means the unit will not accept inbound MP calls.

Example: `MP=No`

Location: Ethernet > Answer > Encaps

See Also: Encaps

MPP

Description: Enables incoming MP+ (Multilink Protocol Plus) connections. MP+ enables the DSL Terminator unit to connect to another DSL Terminator unit using multiple channels.

Usage: Specify Yes or No.

- Yes means the DSL Terminator unit answers MP+ calls, provided that they meet all other connection criteria. Yes is the default.
- No means the DSL Terminator unit will not accept inbound MP+ calls.

Example: `MPP=No`

Location: Ethernet > Answer > Encaps

See Also: Encaps, MP

MRU

Description: Specifies the maximum number of bytes the DSL Terminator unit can receive in a single frame. Usually the default is the right setting, unless the far end requires a lower number.

Third-party devices calculate MRU differently. If you connect to a non-DSL Terminator device, you might need to specify a different MRU to match frame size between the two devices.

Usage: Specify a number lower than the default MRU if the far end requires it.

- In the Answer or a Connection profile, specify a number between 1 and 1524.
- In a Frame Relay profile, specify a number between 128 and 1600.

Example: `MRU=1524`

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options, Ethernet > Frame Relay

See Also: Encaps

Multicast Client

Description: Specifies whether hosts on the other side of the WAN are using IP multicasting. The DSL Terminator unit forwards multicast frames to the interface only if a host with the same group has been detected on this interface.

Usage: Specify Yes or No.

- Yes specifies that hosts on the other side of the WAN are using IP multicasting.
- No specifies that hosts on the other side of the WAN are not using IP multicasting. No is the default.

Example: `Multicast Client=Yes`

Dependencies: This parameter is not applicable if multicast forwarding is disabled or if the Connection profile is the Mbone profile (linking to a remote multicast router). See Multicast Rate Limit for related dependencies.

Location: Ethernet > Connections > IP options

See Also: Multicast Rate Limit

Multicast Grp Leave Delay

Description: Specifies the number of seconds the DSL Terminator unit waits before forwarding an IGMP 2 `leave group` message from a multicast client.

Usage: Specify a number of seconds from 0 to 120. The default is 0 (zero). If you specify a value other than the default, and the DSL Terminator unit receives a `leave group` message, the unit sends an IGMP query to the WAN interface or client from which it received the `leave group` message. If the DSL Terminator unit does not receive a response from an active multicast client that belongs to the client group, it sends a `leave group` message when the time you specify expires.

If you accept the default, the DSL Terminator unit forwards a `leave group` message immediately. If users might establish multiple multicast sessions for identical groups, set Multicast Grp Leave Delay to a value of 10 to 20 seconds.

Example: `Multicast GRP Leave Delay=100`

Dependencies: Multicast Grp Leave Delay applies only if multicast forwarding is enabled.

Location: Ethernet > Connections > IP Options

See Also: Multicast Rate Limit

Multicast Monitor

Description: Specifies whether the system generates a trap when multicast heartbeat monitoring is configured and the system does not receive the configured number of heartbeat packets on a multicast interface.

Usage: Specify Yes or No.

- Yes specifies that the system generates a trap when it does not receive the configured number of heartbeat packets on a multicast interface. The default is Yes.
- No specifies that the system does not generate a trap when it does not receive the configured number of heartbeat packets on a multicast interface.

Example: `Multicast Monitor=No`

Location: Ethernet > SNMP Traps > Enable Traps

Multicast Rate Limit

Description: Specifies the rate at which the DSL Terminator unit accepts multicast packets from clients on this interface. It does not affect the MBONE interface.

Note: By default, the Rate Limit parameter is set to 100. *This disables multicast forwarding on the interface.* The forwarder handles IGMP packets, but does not accept packets from clients or forward multicast packets from the MBONE router.

To begin forwarding multicast traffic on the interface, you must set the rate limit to a number less than 100. For example if you set it to 5, the DSL Terminator unit accepts a packet from multicast clients on the interface every 5 seconds. Any subsequent packets received in that 5-second window are discarded.

Usage: Specify a number lower than the default 100 to begin forwarding multicast traffic on the interface.

Example: `Multicast Rate Limit=5`

Dependencies: This parameter has no effect when applied to the MBONE interface.

Location: Ethernet > Connections > IP Options

See Also: Multicast Client

N

N391

Description: Specifies the interval at which the DSL Terminator unit requests a Full Status Report on a Frame Relay link.

Usage: Specify a number from 1 to 255 seconds. The default is 6.

Example: `N391=15`

Dependencies: This parameter does not apply if FR Type is DCE.

Location: Ethernet > Frame Relay

See Also: Link Mgmt

Nailed Group

Description: Assigns a group number to a T1 or E1 channel.

Usage: Specify a number from 0 to 1024. The default is 0 (zero).

Example: `Nailed Group = 9`

Dependencies: Do not associate a group number with more than one active profile. Channels in a nailed-up group must be contiguous.

Location: Net/8T1 > Line Config > Line *N*, Net/8E1 > Line Config > Line *N*

Nailed-Group

Description: Assigns a group number to an ATM DS3, UDS3, or SDSL line.

Usage: Specify a number from 0 to 1024. The default is 0 (zero).

Dependencies: Do not associate a group number with more than one active profile. Channels in a nailed-up group must be contiguous.

Location: Net/ATM-DS3 > Line Config, Net/UDS3 > Line Config, Net/SDSL-8 > Line Config > Line *N*, Net/SDSL-16 > Line Config > Line *N*

See Also: Activation, Enabled, Line Rate, Rate Mode, TrnkGrp, Unit Type

Nailed Grp

Description: Specifies a number assigned to a group of nailed channels by the Nailed Group parameter. Only one active link can be assigned to use a particular group number.

Usage: Specify the number assigned to nailed T1 bandwidth.

Example: `Nailed Grp=5`

Location: Ethernet > Frame Relay

See Also: Call Type

Name

Description: Specifies the name of a profile, host, or user.

Note: When the Name parameter specifies an existing host, user, the system itself, or a Firewall profile, the name is case sensitive. The name you specify must be unique within the list of profiles of the same type. In addition, Ascend strongly recommends that you do not use the same name for a Name-Password profile and a Connection profile.

Usage: Specify a name. In most profiles, the name can contain up to 16 characters. In the Name-Password profile, Route profile and SNMP Traps profile, the name can contain up to 31 characters.

Example: `Name=PacBell`

Location: Net/8E1 > Line Config, Ethernet > Filters, Ethernet > Static Rtes, System > Security, Ethernet > SNMP Traps, System > Sys Config, Ethernet > Name-Password

NAS Port Type

Description: Determines the type of calls that can be received.

Usage: Specify Analog, Digital, or Any (the default, which specifies both types).

Following are the settings for the RADIUS NAS-Port-Type attribute and the analogous settings for the NAS Port Type parameter:

Attribute setting	Parameter settings
Async	Analog, Any
Sync	Digital, Any
ISDN_Sync	Digital, Any
ISDN_Async_V120	Digital, Any
ISDN_Asyn_V110	Digital, Any
Virtual	Any
ISDN_Async_V32	Digital, Any
ISDN_Async_VDSP	Any

Example: `NAS Port Type = Digital`

Location: Ethernet > Connections > *any Connection profile* > Telco options... > NAS Port Type

Net Adrs

Description: In a Bridge profile, specifies the IP address of a device at the remote end of the link. If you are bridging between two segments of the same IP network, you can use the Net Adrs parameter in a Bridge profile to enable the DSL Terminator unit to respond to ARP

requests while bringing up the bridged connection. If an ARP packet contains an IP address that matches the Net Adrs parameter of a Bridge profile, the DSL Terminator unit responds to the ARP request with the Ethernet (physical) address specified in the Bridge profile and brings up the specified connection. In effect, the DSL Terminator unit as a proxy for the node that actually has that address.

Usage: Specify the IP address of the device on the remote network.

Example: `Net Adrs=10.207.23.101/24`

Location: Ethernet > Bridge Adrs

See Also: Enet Adrs

New NASPort ID

Description: Specifies the format the unit recognizes for the NAS-Port (5) RADIUS attribute.

Usage: Specify one of the following:

- Yes specifies that the DSL Terminator unit recognizes the format that specifies a shelf, slot, line, and channel number.
- No specifies that the DSL Terminator unit recognizes the five-digit format that specifies the type of service in use, and the line and channel number. The default value is No.

Example: `New NASPort ID=Yes`

Location: System > Sys Config

Non-Multicast

Description: Specifies whether all multicast packets are remapped to a directed neighbor address.

Usage: Specify Yes or No.

- Yes specifies that all multicast packets are remapped to a directed neighbor address, enabling adjacencies to form between neighbors. This setting is ignored on Ethernet (a broadcast network). Its use is not recommended for unnumbered interfaces. If you specify it for a non-numbered interface, the DSL Terminator drops the packets.
- No specifies that multicast packets are not remapped to a directed neighbor address. The default is No.

Example: `NonMulticast=yes`

Location: Ethernet > Connections > *any Connection profile* > OSPF options...

No Trunk Alarm

Description: Specifies whether the back panel alarm relay closes when all T1 PRI lines (or trunks) go out of service. The DSL Terminator has an alarm relay whose contacts remain open on the back panel's alarm relay terminal block during normal operation. If you enable them, the alarm relay contacts close during loss of power, hardware failure, or a system reset. The No

Trunk Alarm parameter enables you to specify whether the contacts also close when all T1 PRI lines go out of service.

Usage: Specify Yes or No.

- Yes means the DSL Terminator closes the back panel alarm relay when all trunks go out of service.
- No means the DSL Terminator records the event in the log but does not close the alarm relay. No is the default.

Example: `No Trunk Alarm=yes`

Location: System > Sys Config

NumPlanID

Description: NumPlanID is used for outbound calls made by the DSL Terminator on PRI lines so that the switch can properly interpret the phone number dialed. Ask your PRI provider for details on when to use each of the following settings. This parameter specifies NumberPlanID field in the called party's information element.

Usage: Specify one of the following values:

- Unknown (NumberPlanID=0)
- ISDN (the default) (NumberPlanID=1)
- Private (NumberPlanID=9)
- No is the default.

Example: `NumPlanID=ISDN`

Dependencies: The value you specify for NumPlanID in the Dial Plan profile overrides the value of NumPlanID in the Call profile and Connection profile if you have enabled the unit's Dial Plan profiles.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory (Call profiles), Ethernet > Connections (Connection profiles), System > Dial Plan, Ethernet > Frame Relay, Ethernet > X.25

See Also: PRI # Type, Call-by-Call, T1-PRI:NumPlanID (Line profiles), Modem:NumPlanID (System profile)

Num Trunk Digits

Description: Specifies the maximum number of digits that a trunk-group designation can contain.

Usage: Specify an integer from 1 to 4. The default is 1.

Example: `Num Trunk Digits=3`

Dependencies: You must set Use Trunk Groups=Yes for Num Trunk Digits to apply.

Location: System > Sys Config

See Also: Use Trunk Groups

O

Offset

Description: In a filter of type Generic, specifies a byte-offset from the start of a frame to the data in the packet to be tested against this filter. For example, with this filter specification:

```
Filters
   Name=filter-name
   Input filters...
      In filter 01
         Generic...
            Forward=No
            Offset=2
            Length=8
            Mask=0F FF FF FF 00 00 00 F0
            Value=07 FE 45 70 00 00 00 90
            Compare=Equals
            More=No
```

and the following packet contents:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

The first two byes in the packet (2A and 31) are ignored due to the two-byte offset.

Note: If the current filter is linked to the previous one (if More=Yes in the previous filter), the offset starts at the endpoint of the previous segment.

Usage: Specify a number indicating a byte-offset.

Example: `Offset=2`

Location: Ethernet > Filters > Input filters > In filter *N* > Generic, Ethernet > Filters > Output filters > Out filter *N* > Generic

See Also: Length, Mask, More

Operations

Description: Enables or disables permission to view profiles and to change the value of any parameter. When it is disabled, users can view profiles, but cannot change the value of any parameter (read-only security). In addition, when this permission is disabled, users cannot access most DO commands. Only DO Esc and DO password are available.

Note: If this permission is disabled, all other permissions are disabled as well.

Usage: Specify Yes or No.

- Yes means the operator can view and edit profiles. Yes is the default.
- No disables this permission as well as all other permissions in the Security profile.

Example: `Operations=No`

Location: System > Security

Option

Description: Specifies the criteria the DSL Terminator uses to select a trunk group when it places a call from a Destination profile. Each Destination profile contains six Call-by-Call N and Dial N# parameters. Therefore, you can configure up to six options for reaching the destination device. The Option parameter helps the DSL Terminator select which option to use.

Usage: Specify one of the following values:

- 1st Avail specifies that the DSL Terminator selects the first trunk group that has enough available bandwidth to meet the base bandwidth requirements of the Call profile (as defined by the Base Ch Count parameter).

  If no group has enough bandwidth, the DSL Terminator drops the call.

  1st Avail is the default.

- 1st Active specifies the first trunk group that has at least one available channel.

  If you choose this setting, set the Port profile parameter Fail Action=Reduce so that the DSL Terminator does not disconnect the call even if the full base bandwidth specified by Base Ch Count is not available.

- Any specifies that the DSL Terminator uses any combination of circuits from any trunk group to make the call.

  Note that the DSL Terminator does not allow you to combine channels from trunk groups of different carriers to obtain a full base bandwidth.

Example: `Option=1st Active`

Location: System > Destinations

See Also: B1 Trnk Grp, B2 Trnk Grp, Base Ch Count, Call-by-Call *N*, Ch *N* Trnk Grp, Dial *N*#, Fail Action

Own Port Diag

Description: Enables or disables permission to perform the commands in the Port Diag menu for the AIM port that was called.

Note: To completely disable the operator's ability to perform diagnostics for the called port, you must also disable All Port Diag.

Usage: Specify Yes or No. Yes is the default if All Port Diag is set to No.

- Yes means the operator can use the diagnostic commands in the Port Diag menu for the AIM port that was called. Yes is the default if All Port Diag is set to No.
- No disables this permission.

Example: `Own Port Diag=No`

Dependencies: This parameter is not applicable if the Operations permission is disabled or if All Port Diag is set to Yes.

Location: System > Security

See Also: All Port Diag

P

Parallel Dial

Description: Specifies the number of channels that the DSL Terminator can dial simultaneously over the T1 PRI line, or that the DSL Terminator can disconnect simultaneously. Although you can specify any number of channels, the initial number of channels in a connection never exceeds the value of the Base Ch Count parameter. Similarly, when the DSL Terminator adds or subtracts channels, the values for Max Ch Count and Min Ch Count override any setting for Parallel Dial.

Note: If calls from the U.S. to another country have trouble establishing an initial connection at the full bandwidth, reduce the Parallel Dial parameter to a value of 2 or 1.

Usage: Specify a number between 1 and 12. The default is 5.

Example: `Parallel Dial=8`

Location: System profile: System > Sys Config

See Also: Base Ch Count

Passwd

Description: Specifies the password required to authenticate a Security profile. The first Security profile, Default, has no password.

Note: Passwords are case-sensitive.

Usage: Specify up to 20 characters.

Example: `Passwd=gloriosky`

Location: System > Security

See Also: Edit Security

Password

Description: Specifies the password that an incoming Appletalk Remote Access (ARA) caller must supply (Connection profile) or the password the Foreign Agent must specify under Ascend Tunnel Management Protocol (ATMP) in order to access this unit (Ethernet profile).

Note: Passwords are case-sensitive.

Usage: Specify up to 20 characters.

Example: `Password=gloriosky`

Dependencies: In a Connection profile, Password is not applicable unless Encaps is set to ARA. In the Ethernet profile, Password is not applicable unless ATMP is enabled and the ATMP Mode is Home.

Location: Ethernet > Connections > Encaps Options, Ethernet > Mod Config > ATMP Options

See Also: , ATMP Gateway, ATMP Mode, Encaps, Type, UDP Port

Password Port

Description: Specifies the UDP port number that the APP Server is monitoring.

Usage: Specify a number from 0 to 65535. The default is 0 (zero), which indicates that the APP Server is not monitoring a UDP port.

Example: `Password Port=1699`

Dependencies: Password Port applies only to outgoing calls using security-card authentication. These conditions must apply:

- The DSL Terminator unit must request PAP-Token authentication.
- You must set Password Server=Yes.
- You must have the APP Server utility running on a UNIX or Windows workstation on the local network.

Location: Ethernet > Mod Config > Auth

See Also: Password Server

Password Server

Description: Enables the DSL Terminator unit to respond to security-card password challenges.

Usage: Specify Yes or No.

- Yes specifies that the DSL Terminator unit uses the APP Server utility to password challenges.
- No disables responses from the APP Server utility. The default is No.

Example: `Password Server=Yes`

Dependencies: Password Server applies only to outgoing calls using security-card authentication. These conditions must apply:

- The DSL Terminator unit must request PAP-Token authentication.
- You must set Password Port to a nonzero value..
- You must have the APP Server utility running on a UNIX or Windows workstation on the local network.

Location: Ethernet > Mod Config > Auth

See Also: Password Port

Peak Rate

Description: Specifies the maximum rate at which the virtual circuit using a Traffic Shaping profile transmits data. The DSL Terminator can transmit the number of cells specified in the MAX Burst Size parameter at the peak rate.

Usage: Specify a value (in kilobits per second) from 0 (zero) to the maximum rate the interface supports. For a DS3-ATM card the maximum is 37290; for an OC3-ATM card the maximum rate is 135631. The default is 1000.

Example: `Peak rate=4000`

Dependencies: The Traffic Shaper profile must be enabled for Peak Rate to apply.

Location: Net/DS3-ATM > Line Config > *any line profile* > Traffic Shapers,
Net/OC3-SMF-ATM > Line Config > *any line profile* > Traffic Shapers,
Net/OC3-UTP-ATM > Line Config > *any line profile* > Traffic Shapers

See Also: Aggregate, Bit Rate, , Max Burst Size, Priority, Traffic Shaper

Perm Conn Update

Description: Specifies under what circumstances the DSL Terminator unit performs nonintrusive remote updates of the configurations of permanent connections.

Usage: Specify one of the following values:

- All (the default) specifies that, if they are fetched from the RADIUS server, all existing permanent connections are torn down and reestablished following the update. This setting causes service interruption every time any nailed profile is updated or added.
- Changed specifies that only changed permanent connections are torn down and reestablished.

Example: `Perm Conn Update=Changed`

Location: System > Sys Config

See Also: Use Trunk Grps

Pool

Description: Specifies an IP address pool from which the caller is assigned an IP address. If the Pool parameter is null but all other configuration settings enable dynamic assignment, the DSL Terminator unit gets IP addresses from the first defined address pool.

You can define up to 10 IP address pools in the VT100 interface. RADIUS supports up to 50 address pools.

Usage: Specify the number of the pool. The default is 1.

Example: `Pool=24`

Location: Ethernet > Connections > IP Options

See Also: Assign Adrs, Pool # Count, Pool # Start

Pool #N Count (N=1–10)

Description: Specifies how many IP addresses are in the numbered pool (up to 254). N represents the number of the pool, which can be 1 through 10.

Note: Addresses in a pool do not accept a netmask modifier, because they are advertised as host routes. If you allocate IP addresses on a separate IP network or subnet, make sure you inform other IP routers about the route to that network or subnet.

Usage: For each pool, specify a number between 0 and 254.

Example: `Pool#2 Count=32`

Dependencies: The starting address must be specified in the Pool #N start parameter.

Location: Ethernet > Mod Config > WAN Options

See Also: Pool Only, Pool #N Start

Pool #N Name (N=1-10)

Description: Specifies the name of an IP address pool

Usage: Specify a name. You can enter up to 10 characters. The first character cannot be a number.

Example: `Pool #2=gloriosky`

Location: Ethernet > Mod Config > WAN Options

Pool #N Start (N=1–10)

Description: Specifies the first address in a block of contiguous addresses on the local network or subnet. The Pool#1 Count parameter specifies the number of contiguous addresses in that pool.

Usage: Specify the first IP address in the pool. The address you specify does not need to be on the same LAN segment as the DSL Terminator unit. The default is 0.0.0.0.

Example: `Pool #1 Start=200.207.23.1`

Dependencies: The number of addresses in the pool must be specified in the Pool #N count parameter.

Location: Ethernet > Mod Config > WAN Options

See Also: Pool #N count, Pool only

Pool Chaining

Description: Specifies whether IP pool chaining is enabled. Pool chaining enables the DSL Terminator unit to automatically use the next IP address pool when the current IP address pool is exhausted.

Usage: Specify Yes or No.

- Yes enables pool chaining. The default is Yes.
- No disables pool chaining.

Example: `Pool Chaining=No`

•

Dependencies: A pool chain starts at the first pool definition and stops at a null pool.

Location: Ethernet > Mod Config > WAN Options

See Also: Pool #N Count, Pool #N Start, Pool Only

Pool Only

Description: Instructs the DSL Terminator unit to hang up if a caller rejects the dynamic assignment. During PPP negotiation, a caller may reject the IP address offered by the DSL Terminator unit and present its own IP address for consideration. Connection profiles compare IP addresses as part of authentication, so the DSL Terminator unit would automatically reject such a request if the caller has a Connection profile. However, Name-Password profiles have no such authentication mechanism, and could potentially allow a caller to spoof a local address.

Usage: Specify Yes or No.

- Yes means the caller must accept dynamic assignment. This is recommended if Name-Password profiles are in use.
- No means the DSL Terminator unit allows the caller to reject the IP address offered by the unit and present its own IP address for consideration. No is the default.

Example: `Pool Only=Yes`

Dependencies: At least one address pool must be defined, and addresses must be available.

Location: Ethernet > Mod Config > WAN Options

See Also: Pool # Count, Pool # Start

Pool Summary

Description: Indicates that network summarization is in use.

Network summarization reduces the size of route advertisements by summarizing a series of host routes into a network advertisement. Packets destined for a valid host address on that network are routed to the host, and packets destined for an invalid host address are rejected with an ICMP “host unreachable” message. To use the pool summary feature, create a network-aligned pool and set the Pool Summary parameter to Yes.

To be network-aligned, the Pool Start address must be the first host address. Pool Start address –1 is used to determine the network address (the zero address on the subnet). To have a power of two size, the Pool Count value must be two less than a power of two; for example, 2, 6, 14, 30, 62, 126. The Pool Count value + 2 is used to create a netmask.

For example, with this configuration:

```
Pool Summary=Yes
Pool#1 start=10.12.253.1
Pool#1 count=126
```

The network alignment address is Pool Start address –1: 10.12.253.0 and the netmask is Pool Count +2 addresses: 255.255.255.128. The resulting address pool network is:

```
10.12.253.0/25
```

Usage: Specify Yes or No.

- Yes indicates that network summarization is in use. The Pool Count and Pool Start values must be set up as described above.
- No indicates that host routes will not be summarized. No is the default.

Example: `Pool Summary=Yes`

Dependencies: The Pool Count and Pool Start values must be set up as described above.

Location: Ethernet > Mod Config > WAN Options

See Also: Pool #N Start, Pool #N Count

PPP

Description: Enables incoming PPP (Point-to-Point Protocol) connections. PPP sessions are single-channel connections to any remote device running PPP software.

Usage: Specify Yes or No. Yes is the default.

- Yes specifies that the DSL Terminator unit accepts inbound PPP calls, provided that they meet all other connection criteria. Yes is the default.
- No specifies that the DSL Terminator unit does not accept inbound PPP connections.

Example: `PPP=No`

Location: Ethernet > Answer > Encaps

PPPoE Enable

Description: Specifies whether the unit responds to PPP over Ethernet (PPPoE) packets arriving on the interface or associated with an active Connection profile.

Usage: Specify Yes or No.

- Yes specifies that the unit responds to PPPoE packets arriving on the interface or associated with the Connection profile.
- No specifies that the unit does not respond to PPPoE packets arriving on the interface or associated with the Connection profile. The default is No.

Example: `PPPoE=Yes`

Dependencies: PPPoE Enable is not applicable if bridging is turned off for the interface.

Location: Ethernet > Mod Config > Ether1 Options, Ethernet > Mod Config > Ether2 Options, Ethernet > Connections > PPPoE Options

See Also: Bridge Non PPPoE

PPTP Enabled

Description: Enables or disables Point-to-Point Tunneling Protocol (PPTP) functionality in the DSL Terminator unit. When PPTP is enabled, the DSL Terminator unit can bring up a PPTP tunnel with a PPTP Network Server (PNS) and respond to a request for a PPTP tunnel from a PNS. You must specify the IP address of the PNS in one or more of the Route Line parameters.

Usage: Specify Yes or No.

- Yes enables PPTP, enabling the DSL Terminator unit to bring up a PPTP tunnel to a PNS or respond to a tunnel request.
- No disables PPTP. No is the default.

Example: PPTP=`Yes`

Location: Ethernet > Mod Config > L2 Tunneling Options

See Also: Route Line *N*, Line *N* Tunnel Type

Precedence

Description: Specifies the priority level of the data stream.

Usage: The three most significant bits of the Type-of-Service (TOS) byte are priority bits used to set precedence for priority queuing. When TOS is enabled, you can set those bits to one of the following values (most significant bit first):

- 000 specifies normal priority (the default).
- 001 specifies priority level 1.
- 010 specifies priority level 2.
- 011 specifies priority level 3.
- 100 specifies priority level 4.
- 101 specifies priority level 5.
- 110 specifies priority level 6.
- 111 specifies priority level 7 (the highest priority).

Example: Priority=`010`

Location: Ethernet > Connections > IP Options, Ethernet > Filters > Input filters > In filter *N* > IPTOS, Ethernet > Filters > Output filters > Out filter *N* > IPTOS

See Also: Active, Apply To, Type of Service

Preference

Description: Specifies the preference value for a route. RIP is a distance-vector protocol, which uses a hop count to select the shortest route to a destination network. OSPF is a link-state protocol, which means that OSPF can take into account a variety of link conditions, such as the reliability or speed of the link, when determining the best path to a destination network. Because these two metrics are incompatible, the DSL Terminator unit supports route preferences.

When choosing which routes is put in the routing table, the router first compares preference values, preferring the lower number. If the preference values are equal, then the router compares the metric field, using the route with the lower metric.

- Connected routes have a default preference of 0.
- OSPF routes have a default preference of 10.
- ICMP redirects have a default preference of 30.
- RIP routes have a default preference of 100.
- Static routes have a default preference of 100.
- ATMP routes have a default preference of 100.

Usage: Specify a number between 0 and 255. Zero is the default for connected routes (such as the Ethernet). The value of 255 means *Do not use this route*; this value is meaningful only for Connection profiles.

Example: `Preference=100`

Location: Ethernet > Connections > IP Options, Ethernet > Static Rtes

Preempt

Description: Specifies the number of idle seconds the DSL Terminator waits before using one of the channels of an idle link for a new call.

Usage: Specify a number between 0 and 65535. The DSL Terminator sets no time limit if you enter 0 (zero). The default setting is 60.

Example: `Preemp=200`

Location: Ethernet > Answer > Session Options, Ethernet > Connections > Session Options

See Also: Call Type

PrependDigits

Description: Specifies digits to add in front of an outgoing call.

Example: `PrependDitits=9`

Location: System > Dial Plan >

Pri DNS

Description: Specifies the IP address of the primary domain name server. You can specify a primary and secondary name server of each type. The secondary server is accessed only if the primary one is inaccessible.

Usage: Specify the IP address of the primary domain name server. The default value is 0.0.0.0. Accept this default if you do not have a domain name server.

Example: Pri DNS=10.207.23.1

Location: Ethernet > Mod Config > DNS

See Also: Domain Name, Sec DNS

Priority

Description: Specifies the priority of this router with respect to the designated router and backup designated router (BDR) elections under OSPF. When two routers attached to a network attempt to become the designated router, the one with the highest Priority value takes precedence. A router whose Priority is set to 0 (zero) is ineligible to become the designated router on the attached network.

Usage: Specify a number. The default value is 5.

Example: `Priority=4`

Location: Ethernet > Connections > OSPF Options, Ethernet > Mod Config > OSPF Options

PRI # Type

Description: Description: PRI # Type is used for outbound calls made by the MAX on PRI lines so that the switch can properly interpret the phone number dialed. Ask your PRI provider for details on when to use each of the following settings. This parameter specifies the TypeOfNumber field in the called party's information element.

Usage: Usage: Specify one of the following values:

- National (the default) specifies phone numbers within the U.S. (TypeOfNumber=2)
- Intl specifies phone numbers outside the U.S. (TypeOfNumber=1)
- Local specifies phone numbers within your Centrex group. (TypeOfNumber=4)
- Abbrev. specifies that the phone number is abbreviated. (TypeOfNumber=6)
- NetSpecific (currently not implemented) specifies that the network you are connected to understands the phone number (TypeOfNumber=3)
- Unknown specifies that the phone number is none of the above. (TypeOfNumber=0)
- Inherit (Dial Plan profile only) applies to calls placed by a device connected to a local T1 PRI line supplied by a Host/BRI module. If you choose this setting, the caller on the WAN requests the same TypeOfNumber as the caller on the local ISDN BRI line.

Example: `PRI # Type=4`

Dependencies: The value you specify for PRI # Type in the Dial Plan profile overrides the value of PRI # Type in the Call profile and Connection profile if you have enabled the unit's Dial Plan profiles.

Location: Location: Ethernet >Connections (Connection profiles), System > Dial Plan, Ethernet > Frame Relay, Ethernet >X.25

See Also: See Also: NumPlanID, Call-by-Call, T1-PRI:PRI # Type (Line profiles), Modem:PRI# Type (System profile)

Private

Description: Specifies whether the DSL Terminator unit will disclose the existence of this route when queried by RIP or another routing protocol. Private routes are used internally but are not advertised.

Usage: Specify Yes or No.

- Yes makes the route private. The DSL Terminator unit does not advertise the route.
- No means the route is advertised via routing protocols. No is the default.

Example: `Private=Yes`

Dependencies: This parameter applies only if IP routing is enabled.

Location: Ethernet > Connections > IP Options, Ethernet > Static Rtes

See Also: LAN Adrs, Metric, RIP, Route IP

Pri WINS

Description: Specifies the IP address of the primary Windows INternet Name Server (WINS) server.

Usage: Specify an IP address in dotted decimal notation. The default is 0.0.0.0.

Example: `Pri WINS=10.3.3.100`

Location: Ethernet > Mod Config > DNS

See Also: Sec WINS

Profile Reqd

Description: Specifies whether the DSL Terminator unit rejects incoming calls for which it could find no Connection profile and no entry on a remote authentication server. If you do not require a configured profile for all callers, the DSL Terminator unit builds a temporary profile for unknown callers. Many sites consider this a security breach.

Note: Setting Profile Reqd to Yes disables Guest access for ARA connections.

Usage: Specify Yes or No.

- Yes means a configured profile is required for all callers.

- No means that if a configured profile is not found, the DSL Terminator unit builds a temporary profile for the unknown caller. No is the default.

Example: `Profile Reqd=Yes`

Location: Ethernet > Answer

See Also: , Encaps, Recv Auth, Route IP

Protocol

Description: In a filter of type IP, specifies the protocol number to which the DSL Terminator unit compares a packet's protocol number. If you specify a protocol number, the unit compares it to the protocol number field in packets to match them to this filter. The default protocol number of 0 (zero) matches all protocols. Common protocols are listed below, but protocol numbers are not limited to this list. For a complete list, see the section on Well-Known Port Numbers in RFC 1700, *Assigned Numbers*, by Reynolds, J. and Postel, J., October 1994.

- 1: ICMP
- 5: STREAM
- 8: EGP
- 6: TCP
- 9: Any private interior gateway protocol (such as Cisco's IGRP)
- 11: Network Voice Protocol
- 17: UDP
- 20: Host Monitoring Protocol
- 22: XNS IDP
- 27: Reliable Data Protocol
- 28: Internet Reliable Transport Protocol
- 29: ISO Transport Protocol Class 4
- 30: Bulk Data Transfer Protocol
- 61: Any Host Internal Protocol
- 89: OSPF

In a Static Mapping *N* submenu, Protocol specifies whether the Dst Port # and Loc Port # parameters specify TCP or UDP ports.

Note: If you change the value of Protocol in the Static Mapping *N* submenu, the change does not take effect until the next time a connection is made to the remote network. To make the change immediately, you must terminate the connection to the remote network and then reopen it.

Usage: For a Filter profile, specify the number of the protocol. You can enter a number between 0 and 255. The default setting is 0 (zero). When you accept the default, the DSL Terminator unit disregards the Protocol parameter when applying the filter.

In a Static Mapping *N* submenu, specify one of the following values:

- TCP (the default) specifies that the Dst Port # and Loc Port # parameters in the same Static Mapping *N* submenu are TCP port numbers.

- UDP specifies that the Dst Port # and Loc Port # parameters in the same Static Mapping *N* submenu are UDP port numbers.

Example: `Protocol=UDP`

Dependencies: If the Routing parameter is set to No or the Lan parameter is set to Multi IP Addr, the Protocol parameter is not applicable.

Location: Ethernet > Filters > Input filters > In filter *N* > IP, Ethernet > Filters > Output filters > Out filter *N* > IP, Ethernet > Filters > Input filters > In filter *N* > IPTOS, Ethernet > Filters > Output filters > Out filter *N* > IPTOS

See Also: Type, Valid

Proxy ARP

Description: Specifies under what conditions the DSL Terminator responds to Address Resolution Protocol (ARP) requests for remote devices. When you enable Proxy ARP, the DSL Terminator responds to the ARP request with its own Media Access Control (MAC) address. Typically, Proxy ARP is enabled when the following conditions exist:

- The DSL Terminator-supplied IP addresses are in the same local subnet as the DSL Terminator.
- Hosts on the local subnet must send packets to the remote clients.

You normally do not need to enable Proxy ARP, because most routing protocols (including those used over the Internet) are designed to propagate subnet mask information.

Usage: Specify Yes or No.

- No disables proxy ARP. The default is No.
- Yes specifies that the DSL Terminator responds to an ARP request with its own MAC address if the ARP request is sent to a host to which the DSL Terminator has a route.

Example: `Proxy ARP=yes`

Dependencies: Keep this additional information in mind.

- This parameter does not apply if Enabled is set to No in the BIR Options submenu.
- This parameter does not apply if IP routing is not enabled.

Location: Ethernet > Mod Config > Ether Options

See Also: Enabled (BIR), Bridge Group

Proxy Mode

Description: Specifies under what conditions the DSL Terminator unit responds to ARP requests for remote devices. When you enable Proxy Mode, the unit responds to the ARP request with its own MAC address.

Typically, Proxy ARP is enabled when the DSL Terminator unit supplies IP addresses dynamically to dial-in hosts, and both of the following conditions exist:

- The unit-supplied IP addresses are in the same local subnet as the DSL Terminator unit

- Hosts on the local subnet must send packets to the dial-in hosts.

You normally do not need to enable Proxy ARP, because most routing protocols (including those used over the Internet) are designed to propagate subnet mask information.

Usage: Specify one of the following values:

- Off disables proxy ARP. This is the default.
- Always specifies that the DSL Terminator unit responds to an ARP request with its own MAC address if the ARP request is sent to a host to which the DSL Terminator unit has a route.
- Active specifies that the DSL Terminator unit responds to an ARP request with its own MAC address if the ARP request is sent to a host to which the DSL Terminator unit has an active connection.
- Inactive specifies that the DSL Terminator unit responds to an ARP request with its own MAC address if the ARP request is sent to a host to which the DSL Terminator unit has an inactive connection.

  Note: Proxy ARP does not apply to inactive user profiles stored in RADIUS.

Example: `Proxy Mode=Always`

Dependencies: This parameter applies only if IP routing is enabled.

Location: Ethernet > Mod Config > Ether Options

See Also: Net Adrs, Route IP

Q

Queue Depth

Description: Specifies the queue depth for Simple Network Management Protocol (SNMP) requests.

Usage: Specify a number from 0 to 1024. The default is 0 (zero), which means that the DSL Terminator unit does not drop packets, no matter how far behind the SNMP subsystem gets. If the queue grows too large in a heavily loaded routing environment, the system can ultimately run out of memory.

Example: `Queue Depth=500`

Location: Ethernet > Mod Config > SNMP Options

See Also: RIP Queue Depth

R

RADIUS Change

Description: Specifies whether the system generates a trap when a new RADIUS server is being accessed. This trap returns the objectID and IP address of the new server.

Usage: Specify Yes or No.

- Yes specifies that the system generates a trap when a new RADIUS server is being accessed.The default is Yes.
- No specifies that the system does not generate a trap when a new RADIUS server is being accessed.

Example: `RADIUS Change=No`

Location: Ethernet > SNMP Traps > Enable Traps

See Also: Configuration Change

Rate Limit

Description: Specifies the rate at which the DSL Terminator unit accepts multicast packets from clients on this interface. It does not affect the MBONE interface.

Note: By default, the Rate Limit parameter is set to 100. *This disables multicast forwarding on the interface.* If multicast forwarding is enabled on the interface but the Rate Limit parameter is left at the default 100, the forwarder handles IGMP packets, but does not accept packets from clients or forward multicast packets from the MBONE router.

To begin forwarding multicast traffic on the interface, you must set the rate limit to a number less than 100. For example if you set it to 5, the DSL Terminator unit accepts a packet from multicast clients on the interface every 5 seconds. Any subsequent packets received in that 5-second window are discarded.

Usage: Specify a number lower than the default 100 to begin forwarding multicast traffic on the interface.

Example: `Multicast Rate Limit=5`

Dependencies: This parameter has no effect when applied to the MBONE interface.

Location: Ethernet > Mod Config > Multicast

See Also: Multicast Forwarding, Mbone Profile, Client, Multicast Rate Limit

Example: `Rate Mode=Autobaud`

Read Comm

Description: Specifies a read-only SNMP community name. If an SNMP manager sends this community name, it can access the Get and Get-Next SNMP agents.

Usage: Specify the community name that the DSL Terminator unit uses for authenticating the SNMP management station for read-only access. You can enter up to 16 alphanumeric characters. The default is Public.

Example: `Read Comm=Admin`

Location: Ethernet > Mod Config > SNMP Options

See Also: R/W Comm, R/W Comm Enable

Realm Delimiters

Description: Specifies the characters that delimit a realm from the user name.

Usage: Specify up to seven characters in any order. The default is `@\/%`. If you do not specify any characters, the system behaves as though Keep User Name=Change Name.

Example: `Realm Delimiters=%`

Dependencies: The Realm Delimiters setting does not apply unless Keep User Name is set to Keep Realm.

See Also: Keep User Name

Recv Auth

Description: Specifies the authentication protocol that the DSL Terminator unit uses to receive and verify a password for an incoming PPP connection.

Usage: Specify one of the following values:

- None (the default) means the DSL Terminator unit does not use an authentication protocol to validate incoming calls.
- PAP indicates the Password Authentication Protocol.

  PAP provides a simple method for a host to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption. The remote device must support PAP.
- CHAP indicates the Challenge Handshake Authentication Protocol.

  CHAP is more secure than PAP. It provides a way to periodically verify the identity of a host using a three-way handshake and encryption. Authentication takes place upon initial link establishment; the DSL Terminator unit can repeat the authentication process any time after the connection is made. The remote device must support CHAP.
- MS-CHAP means the connection must use Microsoft's extension of CHAP. MS-CHAP was designed mostly for Windows NT/Lan Manager platforms.
- Either specifies any of the supported authentication schemes.

  When you select Either, the DSL Terminator unit allows authentication if the remote peer can authenticate using any of the designated authentication schemes.

Example: `Recv Auth=CHAP`

Dependencies: f you specify an authentication method, you must also specify a password in the caller’s profile. For a nailed connection, you must set Recv Auth and Send Auth to the same value at both ends of the connection.

Location: Ethernet > Answer > PPP Options

See Also: Auth Host, Lan, Recv PW, Send Auth, Send PW

Recv PW

Description: Specifies the password that the DSL Terminator unit expects to receive from the far end while the connection is being authenticated. If this password is not sent by the far end device, authentication fails.

Usage: Specify a password, up to 20 characters. The password is case sensitive. The default is null.

Example: `NumPlanID=ISDN`

Example:

Dependencies: This parameter does not apply if Recv Auth is set to None.

Location: Ethernet > Connections > Encaps Options, Ethernet > Names / Passwords

See Also: Encaps, Recv Auth, Send Auth, Send PW

Remote Mgmt

Description: Specifies whether the operator at the far end of an AIM call can manage the DSL Terminator remotely using the DO Beg/End Rem Mgm command. In remote management, the DSL Terminator uses bandwidth between sites over the management subchannel established by the AIM protocol. If remote management is disabled and the remote operator attempts to invoke that DO command, the message “Remote Management Denied” is displayed.

Usage: Specify Yes or No.

- Yes allows remote management of the DSL Terminator unit via AIM call. Yes is the default.
- No prevents remote management.

Example: `Remote Mgmt=No`

Dependencies: This parameter applies only when Call Type is set to AIM, FT1-B&O, or FT1-AIM. It does not apply if Call Mgm=Static.

Location: System > Sys Config

See Also: Call Mgm, Call Type

Reply DirectedBcast Ping

Description: Specifies whether the DSL Terminator unit forwards directed broadcast traffic to the Ethernet interface.

Usage: Specify Yes or No.

- Yes directs the DSL Terminator unit to forward directed broadcast traffic. Yes is the default.
- No directs the DSL Terminator unit to drop directed broadcast packets, preventing them from propagating to intermediary networks.

Example: `Reply DirectedBcast Ping=No`

Dependencies: Reply DirectedBcast Ping applies only if the DSL Terminator unit supports IP routing.

Location: Ethernet > Mod Config

See Also: Forward Directed Bcast

Reply Enabled

Description: Specifies whether the DSL Terminator unit processes DHCP packets and acts as a DHCP server on this connection.

Usage: Specify Yes or No.

- Yes specifies that the DSL Terminator unit will process DHCP packets.
  If the connection to the DSL Terminator unit is over a bridged connection, the unit responds to all DHCP requests. If the connection is over any other type of connection, the unit responds only to Network Address Translation (NAT) DHCP packets.
- No specifies that the DSL Terminator unit will not process DHCP packets; it routes or bridges DHCP packets as any other packet. No is the default.

Example: `Reply Enabled=Yes`

Location: Ethernet > Answer > DHCP options, Ethernet > Connections > DHCP options

Reset

Description: Specifies whether the DSL Terminator unit is to be reset. Reset reloads the configuration present in NVRAM and brings the unit back up.

Usage: Specify 0 or 1:

- `0` exits to the previous profile.
- `1` starts the system reset

Example: `Reset = 1`

Location: System>Sys Diag>Sys Reset

Reset TImeout

Description: Specifies the number of seconds that must elapse before the DSL Terminator unit returns to using the primary call-logging host (Host #1).

Usage: Specify the number of seconds. The default is 0 (zero), which specifies that the DSL Terminator unit does not return to using the primary call-logging host.

Example: `Reset Timeout=24`

Dependencies: For Reset Timeout to apply, you must set Call Log=Yes and specify at least one value for Host #*N*.

Location: Ethernet > Mod Config > Call Logging

See Also: Acct-ID Base, Allow Stop Only, Call Log, Call Log Timeout, Dst Port, Host # N, Key, Max Retry

Reuse Addr Timeout

Description: Specifies the number of minutes to lease the IP address obtained during DHCP negotiation when Reuse Last Addr=Yes. During the specified time period, the same address is associated with the WAN connection each time it is re-established (even if the WAN session is idle and times out).

Usage: Specify the number of minutes from 0 to 1440 (24 hours). The default is 0 (zero), which disables the timer.

Example: `NumPlanID=ISDN`

Location: Ethernet > NAT > NAT

See Also: Def Server, FR Address, Lan, Profile, Reuse last Addr, Routing

Reuse Last Addr

Description: Specifies whether the last IP address given by the DHCP server is reused in subsequent DHCP negotiations (for the duration specified in the Reuse Addr Timeout parameter).

Usage: Specify Yes or No. The default is No.

- Yes when you need to use the same IP address for TCP applications that do not time out, such as Telnet.
- No—if session is idle for a long enough period of time, it will time out, and the next time the WAN session is established, a new IP address will be assigned by the DHCP server. The default is No.

Example: `Reuse Last Addr=Yes`

Dependencies: Reuse Last Addr is not applicable if NAT routing is disabled, or if multiple-address NAT is in use. In addition, if the original IP address given during DHCP negotiation is lost, and cannot be reused, applications requiring the same IP address must be reset.

Location: Ethernet > NAT > NAT

See Also: Def Server, FR Address, Lan, Profile, Reuse Addr Timeout, Routing

RIP

Description: Specifies how the DSL Terminator unit handles RIP update packets on the interface.

Note: DSL Terminator recommends that all routers and hosts run RIP-v2 instead of RIP-v1. The IETF has voted to move RIP version 1 into the *historic* category and its use is no longer recommended.

Usage: Specify one of the following values:

- Off specifies that the DSL Terminator unit does not transmit or receive RIP updates. Off is the default.
- Recv-v2 indicates that the DSL Terminator unit receives RIP-v2 updates on the interface but does not send RIP updates.
- Send-v2. This setting indicates that the DSL Terminator unit sends RIP-v2 updates on the interface but does not receive RIP updates.
- Both-v2 means the DSL Terminator unit sends and receives RIP-v2 updates on the interface.
- Recv-v1 indicates that the DSL Terminator unit receives RIP-v1 updates on the interface but does not send RIP updates.
- Send-v1. This setting indicates that the DSL Terminator unit sends RIP-v1 updates on the interface but does not receive RIP updates.
- Both-v1 means the DSL Terminator unit sends and receives RIP-v1 updates on the interface.

Example: `RIP=Send-v2`

Dependencies: This parameter applies only if the DSL Terminator unit routes IP.

Location: Ethernet > Answer > Session Options, Ethernet > Connections > IP Options, Ethernet > Mod Config > Ether Options

See Also: Route IP

RIP2 Use Multicast

Description: Enables or disables the default RIP-v2 behavior of using the multicast address (224.0.0.9) to send and receive updates.

Usage: Specify Yes or No. The default is Yes.

- Yes enables RIP-v2 to use the multicast address (224.0.0.9) instead of the broadcast address for its updates. The default is Yes.
- No disables the use of the multicast address for RIP updates. The updates revert to the use of the broadcast address. Use this setting if you must use the broadcast address for backward compatibility with other systems.

Example: `RIP2 Use Multicast=No`

Dependencies: The RIP2 Use Multicast setting does not apply to RIP-v1.

Location: Ethernet > Mod Config > Ether Options

RipASEType

Description: Specifies how RIP routes are propagated into OSPF.

Usage: Specify one of the following values:

- Type1 is a metric expressed in the same units as the link-state metric (the same units as interface cost).
- Type2 is considered larger than any link-state path. Type2 is the default. It assumes that routing between autonomous systems is the major cost of routing a packet, and eliminates the need for conversion of external costs to internal link-state metrics.

Example: `RipASEType=Type1`

Dependencies: This parameter applies only if the DSL Terminator unit routes OSPF.

Location: Ethernet > Mod Config > Route Pref

RIP Policy

Description: Specifies a split-horizon or poison-reverse policy to handle update packets that include routes that were received on the same interface on which the update is sent. Split-horizon means that the DSL Terminator unit does not propagate routes back to the subnet from which they were received. Poison-reverse means that the unit propagates routes back to the subnet from which they were received with a metric of 16.

Usage: Specify Split Hrzn or Poison Rvrs. Poison Rvrs is the default.

Example: `RIP Policy=Poison Rvrs`

Dependencies: This parameter does not apply to RIP-v2. It applies only to RIP-v1 packets.

Location: Ethernet > Mod Config

Rip Preference

Description: Specifies the preference value for routes learned from the RIP protocol.

When choosing which routes to put in the routing table, the router first compares the Rip Preference values, preferring the lower number. If the Rip Preference values are equal, the router compares the Metric values, using the route with the lower Metric.

Usage: Specify a number between 0 and 255. The default value is 100. Zero is the default for connected routes (such as the Ethernet). The value of 255 means *Do not use this route*.

Example: `Rip Preference=100`

Dependencies: These are the default values for other types of routes:

- Routes learned from OSPF=10

- Routes learned from ICMP Redirects=30
- Static routes from IP address pools and RADIUS authentication=100
- Static routes in an IP Route profile or Connection profile=100

Location: Ethernet > Mod Config > Route Pref

Rip Queue Depth

Description: The maximum number of unprocessed RIP requests that the DSL Terminator unit saves. If RIP requests arrive at a rate faster than they can be processed, then a backlog builds up. This parameter sets the maximum depth of the queue. If the queue fills, further packets destined for it are discarded. This limit applies to each RIP socket, so if RIP is running on multiple interfaces, this parameter limits the number of requests stored per interface.

Usage: Enter an integer value from 0 to 1024. If you enter 0, the DSL Terminator unit saves RIP requests until it runs out of memory. The default is 50.

Note: Setting RIP Queue Depth to 0 is not recommended. An unlimited queue depth can result in an out-of-memory error on the DSL Terminator unit if it receives a flood of packets on its RIP port.

Example: `Rip Queue Depth=40`

Dependencies: This parameter does not apply if the unit does not listen to RIP updates.

Location: Ethernet > Mod Config > Route Pref...

See Also: RIP

RIP Summary

Description: Specifies whether to summarize subnet information when advertising routes. If the DSL Terminator unit summarizes RIP routes, it advertises a route to all the subnets in a network of the same class; for example, the route to 200.5.8.13/28 (a class C address) would be advertised as a route to 200.5.8.0. When the DSL Terminator unit does not summarize information, it advertises each route in its routing table without summarizing it—in our example, the unit advertises a route only to 200.5.8.13.

Usage: Specify Yes or No.

- Yes causes the DSL Terminator unit to summarize RIP-v1 subnet information. Yes is the default.
- No means the DSL Terminator unit advertises each route as-is.

Example: `RIP Summary=No`

Dependencies: This parameter does not apply to RIP-v2. It applies only to RIP-v1 packets. In addition, note that RIP Summary does not affect host routes.

Location: Ethernet > Mod Config

Example: `Rip Tag=c0000042`

RIP Trigger

Description: Specifies whether the IP router tags routes that have been updated in the routing table and sends updates that include only the changed routes.

Usage: Specify Yes or No.

- Yes specifies that the router tags changes to its routing table and includes only the tagged routes in its next update. Changes occur when a call arrives or disconnects, RIP or OSPF learns a route from another router, or the administrator modifies a route-related profile. The router broadcasts updates 5 to 8 seconds after the first change in the routing table is detected. The delay helps to prevent constant updates during peak traffic conditions. The result is reduced processing overhead in the router as well as its neighbors. The default is Yes.
- No specifies that the router sends full table updates every 20 to 40 seconds. The full table update is no longer broadcasted at fixed 30-second intervals, to prevent RIP routers on a network from synchronizing and sending large updates in unison.

Example: `RIP Trigger=No`

Location: Ethernet > Mod Config

See Also: RIP

Route AppleTalk

Description: This parameter enables or disables the routing of AppleTalk data packets on the interface. AppleTalk routing must be set on both sides of the connection, and the parameter in the AppleTalk options submenu for the profile.

Usage: Specify Yes or No.

- Yes enables AppleTalk routing.
- No means the DSL Terminator unit does not route AppleTalk for this connection (if set in the Connection profile) or accept inbound AppleTalk routing calls (if set in the Answer profile). No is the default

Example: `Route Apple Talk=Yes`

Location: Ethernet > Answer > PPP Options, Ethernet > Connections

See Also: AppleTalk, AppleTalk Router, Net End, Net Start, Route AppleTalk, Zone Name

Route IP

Description: Enables or disables the routing of IP data packets on the interface. IP routing must be enabled on both sides of the connection, and the DSL Terminator unit must be configured with an IP address in the Ethernet profile. To establish an inbound connection, IP routing must also be enabled in the Answer profile.

Usage: Specify Yes or No.

- Yes enables IP routing. Yes is the default.
- No means the DSL Terminator unit will not route IP for this connection (if set in the Connection profile) or accept inbound IP routing calls (if set in the Answer profile).

Example: `Route IP=No`

Location: Ethernet > Answer > PPP Options, Ethernet > Connections

See Also: Bridge, Encaps, Profile Reqd

Route Line *N*

Description: Specifies the IP address of the L2TP Network Server (LNS) if you set Line *n* tunnel type to L2TP, or the IP address of the PPTP Network Server (PNS) if you set Line *n* tunnel type to PPTP.

Usage: Specify an IP address. The default is 0.0.0.0. If you accept the default, the DSL Terminator unit does not tunnel any call received on the WAN line specified in Line *n* tunnel type.

Example: `Route Line 1=10.10.10.10`

Dependencies: When configuring L2TP, Route line *n* applies only if you set L2TP Mode to LAC or Both. When configuring PPTP, Route line *n* applies only if you set PPTP Enabled to Yes. You must also set the corresponding Line *n* tunnel type parameter to PPTP or L2TP, as applicable.

Location: Ethernet > Mod Config > L2 Tunneling Options

See Also: L2TP Mode, PPTP Enabled, Line *n* tunnel type

Example: `Run OSPF=Yes`

R/W Comm

Description: Specifies a read/write SNMP community name. If an SNMP manager sends this community name, it can access the Get, Get-Next, and Set SNMP agents.

Usage: Specify the community name that the DSL Terminator unit uses for authenticating the SNMP management station for read-write access. You can enter letters and numbers, up to a limit of 16 characters. The default is Write.

Example: `R/W Comm=Admin`

Location: Ethernet > Mod Config > SNMP Options

See Also: Read Comm, R/W Comm Enable

R/W Comm Enable

Description: Enables and disables the use of SNMP Set commands.

Usage: Press Enter to select Yes or No.

- Yes enables the use of SNMP Set commands. To use a set command, you must know the SNMP read-write community string specified in the R/W Comm parameter. Yes is the default.
- No disables the use of set commands.

Example: `R/W Comm Enable=Yes`

Location: Ethernet > Mod Config > SNMP Options

See Also: R/W Comm, Read Comm

RX-Data-Rate-Limit

Description: Specifies the maximum data rate (in k-bits per second) to be received across the connection. You can use this setting to limit bandwidth for a connection according to the rate charged for the account.

Usage: Specify a number from 0 to 64000. The default is 0 (zero), which disables the data-rate limit feature. If the value you specify is larger than the actual bandwidth provided by the line, the connection behaves as though the data rate limit were disabled, except that additional computations are performed unnecessarily.

Example: `set rx-data-rate-limit=32000`

Dependencies: The system activates configurable receive data-rate limits only for connections that use CAP-RADSL, SDSL, and unchannelized DS3 cards. If you specify a value for a connection that does not use these cards, the system ignores the settings.

Location: Connection > Session-Options

See Also: R/W Comm

S

Sec DNS

Description: Specifies the IP address of the secondary domain name server. It is accessed only if the primary DNS server is unavailable.

Usage: Specify the IP address of the secondary domain name server. The default is 0.0.0.0. Accept this default if you do not have a secondary domain name server.

Example: `Sec DNS=200.207.23.1`

Location: Ethernet > Mod Config > DNS

See Also: Domain Name, Pri DNS

Sec Domain Name

Description: Specifies a secondary domain name that the DSL Terminator unit can search using DNS. The DSL Terminator unit performs DNS lookups in the domain configured in Domain Name first, and then in the domain configured in Sec Domain Name.

Usage: Specify a secondary domain name. You can enter up to 63 characters.

Example: `Sec Domain Name=xyz.com`

Location: Ethernet > Mod Config > DNS

See Also: Domain Name

Sec History

Description: Specifies a number of seconds to use as the basis for calculating average line utilization (ALU). The ALU is used in calculating when to add or subtract bandwidth from a multi-channel call that supports dynamic bandwidth management. The number of seconds you choose for the Sec History parameter depends on your device's traffic patterns. For example, if you want to average spikes with normal traffic flow, you may want the DSL Terminator to establish a longer historical time period. If, on the other hand, traffic patterns consist of many spikes that are short in duration, you may want to specify a shorter period of time; doing so assigns less weight to the short spikes. If you specify a small value for the Sec History parameter, and increase the values of the Add Pers parameter and the Sub Pers parameter relative to the value of Sec History, the system becomes less responsive to quick spikes. The easiest way to determine the proper values for Sec History, Add Pers, and Sub Pers is to observe usage patterns; if the system is not responsive enough, the value of Sec History is too high.

Usage: Specify a number between 1 and 300. The default value for MP+ calls is 15 seconds; the default value for dynamic AIM calls is 30 seconds.

Example: `Sec History=200`

Dependencies: This parameter applies only to multilink calls that support dynamic management.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options

See Also: Add Pers, Call Mgm, Dec Ch Count, Dyn Alg, Encaps, Inc Ch Count, Sub Pers,Target Util

SecurID DES Encryption

Description: Specifies whether the server uses standard DES or the native encryption provided by SecurID.

Usage: Specify Yes or No.

- Yes means the server uses standard DES encryption.
- No means the server uses the native encryption provided by SecurID. No is the default.

Example: `SecurID DES Encryption=Yes`

Dependencies: This parameter does not apply unless Auth specifies SECURID.

Location: Ethernet > Mod Config > Auth

See Also: Auth, SecurID Host Retries, SecurID NodeSecret

SecurID Host Retries

Description: Specifies the number of times the DSL Terminator unit attempts to contact the SecurID host before timing out.

Usage: Specify an integer. The default value is 3.

Example: `Securid Host Retries=4`

Dependencies: This parameter does not apply unless Auth specifies SECURID.

Location: Ethernet > Mod Config > Auth

See Also: Auth, SecurID DES Encryption, SecurID NodeSecret

SecurID NodeSecret

Description: The SecurID NodeSecret parameter pecifies that on the first successful authentication attempt, the SecurID host informs the DSL Terminator unit of this secret value, theoretically stored only on the DSL Terminator unit, to be used in subsequent interactions between the DSL Terminator unit and the SecurID host. The operator must have sufficient permissions in the active Security profile to view the value of this parameter.

Note: After the SecurID server sets the value of this parameter, if you later reset the parameter to null, you must reinitialize the interface to the DSL Terminator unit in the SecurID server by using the *Client Edit* menu selection in the ACE server's *sdadmin* utility. Then, the server sends a new NodeSecret at the next successful authentication.

Usage: The initial value must be null (the default). After the first SecurID authentication occurs, the value is set by the server.

Example: `SecurID Node Secret=gloriosky`

Dependencies: This parameter does not apply unless Auth specifies SECURID.

Location: Ethernet > Mod Config > Auth

See Also: Auth, SecurID Host Retries, SecurID NodeSecret

Security

Description: Enables or disables a kind of security, which differs depending on where the parameter appears.

Usage:

For SNMP address security,

- Yes means the DSL Terminator unit compares the source IP address of packets containing SNMP commands against a list of qualified IP addresses. (The DSL Terminator unit always checks the version and community strings before making source IP address comparisons. The Security parameter does not affect those checks.)
- No means the DSL Terminator unit does not compare IP addresses, so address security is not used. For SNMP address security, the default is No.

For SNMP traps,

- Yes means the DSL Terminator unit will generate traps for Security events (such as failed login attempts) and send the trap-PDU to the SNMP manager.
- No means Security events will not generate traps. The default is No.

Example: `Security=Yes`

Location: Ethernet > Mod Config > SNMP Options, Ethernet > SNMP Traps

See Also: Initial Scrn, Passwd, Toggle Scrn

Sec WINS

Description: Specifies the IP address of the secondary NetBIOS server.

Usage: Specify an IP address. The default is 0.0.0.0.

Example: `Sec WINS=10.3.3.100`

Location: Ethernet > Mod Config > DNS

See Also: Pri WINS

Send Auth

Description: Specifies the authentication protocol that the DSL Terminator unit uses to send a password to the far end of a PPP connection.

Usage: Specify one of the following values:

- None (the default) means the DSL Terminator unit does not use an authentication protocol to validate incoming calls.
- PAP indicates the Password Authentication Protocol.

PAP provides a simple method for a host to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption. The remote device must support PAP, and you must specify a password in the Send PW parameter.

- CHAP indicates the Challenge Handshake Authentication Protocol.

  CHAP is more secure than PAP. It provides a way to periodically verify the identity of a host using a three-way handshake and encryption. Authentication takes place upon initial link establishment; the DSL Terminator unit can repeat the authentication process any time after the connection is made. The remote device must support CHAP, and you must specify a password in the Send PW parameter.

- PAP-TOKEN is an extension of PAP authentication.

  In PAP-TOKEN, the user making outgoing calls from the DSL Terminator unit authenticates his or her identity by entering a password derived from a hardware device, such as a hand-held security card. The DSL Terminator unit prompts the user for this password, possibly along with a challenge key. The Network Access Server (NAS) obtains the challenge key from a security server that it accesses through RADIUS.

- PAP-TOKEN-CHAP is PAP-TOKEN for the base channel with CHAP for subsequent channels. For multilink PPP calls where the answering unit requires security card authentication, PAP-TOKEN and PAP-TOKEN-CHAP begin identically when authenticating the first channel of an MP+ call. However, when the DSL Terminator unit adds additional channels to the MP+ call, PAP-TOKEN requires security-card authentication for each new channel, while PAP-TOKEN-CHAP uses CHAP authentication for all new channels. CHAP authentication works automatically, without the use of a hand-held security card.

  If you specify PAP-TOKEN-CHAP, you must enter a password in the Aux Send PW parameter; this password must match the password in the RADIUS entry for authenticating the call. If you do not enter identical passwords in the Aux Send PW parameter and the RADIUS entry, the DSL Terminator unit cannot extend the MP+ call beyond a single channel.

- CACHE-TOKEN begins authentication using a hand-held security card, and fills a token cache set up for you on the RADIUS server.

  CHAP authenticates your subsequent calls without using your hand-held security card. After a period of time configured in your entry in the RADIUS users file, the token cache expires and the next call you place must again be authenticated with your hand-held security card.

  If you request CACHE-TOKEN, the Send PW parameter must match the Ascend-Receive-Secret attribute in the RADIUS entry that authenticated the call. If you do not enter identical passwords in the Send PW parameter and Ascend-Receive-Secret attribute, CACHE-TOKEN calls are rejected after initial access through hand-held security card authentication.

Example: `Send Auth=CHAP`

Dependencies: For a nailed connection, you must set Recv Auth and Send Auth to the same value at both ends of the connection. PAP-TOKEN and PAP-TOKEN-CHAP require configuration of a SAFEWORD or ACE entry in the NAS's RADIUS users file with the caller's name.

Location: Ethernet > Connections > Encaps Options

See Also: Call Type, Dial Brdcast, Encaps, Recv Auth, Recv PW, Send PW

Send Name

Description: Specifies the name that the DSL Terminator unit sends to the far end device during PPP authentication.

Usage: Specify up to 16 characters. The default is null.

Example: `Send Name=Myconnectname`

Dependencies: Authentication fails under the following circumstances:

- The name does not match the string that the far end device expects.
- The password or IP address for the Connection profile does not match the value that the far end device expects.

Location: Ethernet > Connections > Encaps Options

Send PW

Description: Specifies the password that the DSL Terminator unit sends to the far end while the connection is being authenticated. If this password is not received by the far end device, authentication fails.

Usage: Specify a password, up to 20 characters. The password is case sensitive. The default is null.

Example: `Send PW=gloriosky`

Dependencies: This parameter does not apply if Send Auth is set to None.

Location: Ethernet > Connections > Encaps Options

See Also: Encaps, Recv Auth, Recv PW, Send Auth

Serial

Description: Specifies an ISDN subaddress associated with the DSL Terminator unit's AIM ports. ISDN subaddressing is used for routing inbound calls to the appropriate destination in the DSL Terminator unit.

Usage: Specify a number between 0 and 99. The default is 0.

Example: `Serial=67`

Location: System > Sys Config

See Also: Ans *N*#

Server

Description: Enables or disables the on-board RADIUS server, or specifies the IP address of a BOOTP server, depending on where the parameter appears.

In the RADIUS Server submenu of the Ethernet profile, it enables or disables the on-board RADIUS server, which enables the DSL Terminator unit to appear as a server to some client requests.

In the BOOTP Relay submenu of the Ethernet profile, this parameter specifies the IP address of a BOOTP server for handling BOOTP requests. If a server is on the same LAN as the DSL Terminator unit, BOOTP requests from other networks are relayed to the server. If a server is on another network, BOOTP requests from clients on the same LAN as the DSL Terminator unit are relayed to the remote server. If you specify two BOOTP servers, the DSL Terminator unit that relays the BOOTP request determines when each server is used. The order of the BOOTP servers in the BOOTP Relay menu does not necessarily determine which server is tried first.

Usage: To enable the on-board RADIUS server, specify Yes. The default setting is No. To enable the DSL Terminator unit to communicate with a BOOTP server, specify the server's IP address. The default is 0.0.0.0.

Example: `Server=Yes`

Location: Ethernet > Mod Config > RADIUS Server, Ethernet > Mod Config > BOOTP Relay

See Also: BOOTP Relay Enable, Server Key, Server Port

Server Key #N (N=1–9)

Description: Specifies up to nine RADIUS server keys, shared with the RADIUS clients. This parameter is used to validate the authenticator field on requests and generate the authenticator on responses.

Usage: Specify a string containing the shared secret. You can enter up to 20 characters. For security purposes, the string is hidden when the parameter is displayed. The default is null.

Example: `Server Key #2=gloriosky`

Dependencies: This parameter does not apply if the on-board RADIUS server is disabled.

Location: Ethernet > Mod Config > RADIUS Server

See Also: Server, Server Port

Example: `Server Name=Serverfirst`

Server Port

Description: This parameter indicates the UDP port number to use for the on-board RADIUS server.

Usage: Specify a number between 1 and 65535. The default is 1700. Although the value can match the port setting for RADIUS authentication or accounting, Lucent recommends that you specify a different port.

Example: `Server Port=1453`

Dependencies: This parameter does not apply if the on-board RADIUS server is disabled.

Location: Ethernet > Mod Config > RADIUS Server

See Also: Server, Server Key

Example:

Ses-Line-Rate

Description: Specifies the symmetrical data rate.

Usage: Specify one of the following values:

144000
272000
400000
528000
784000
1168000
1552000

Example: `Ses-Line-Rate=272000`

Location: Ethernet > Connections > Session-Options

Session Key

Description: Specifies whether or not all new session entries are assigned a session key in RADIUS.

Usage: Specify Yes or No.

- Yes means session keys are assigned to all new session entries.
- No means session keys are not assigned. No is the default.

Example: `Session Key=Yes`

Dependencies: This parameter is not applicable if Server is set to No.

Location: Ethernet > Mod Config > RADIUS Server

Sess Timer

Description: When set for RADIUS accounting, this parameter sets the amount of time the DSL Terminator unit waits for a response to a RADIUS Accounting Request. You can set this parameter globally and for each connection. If it does not receive a response within that time, the DSL Terminator unit sends the Accounting Request to the next server's address (for example, server #2). If all RADIUS accounting servers are busy, the DSL Terminator unit stores the Accounting Request and tries again at a later time. It can queue up to 154 requests.

When set for RADIUS/LOGOUT authentication, Sess Timer specifies the interval at which session reports are sent to the RADIUS/LOGOUT authentication server. For example, if you wish the DSL Terminator unit to send Session Events at 1-minute (60-second) intervals, set Auth to RADIUS/LOGOUT and Sess Timer to 60.

Usage: When setting the timer for RADIUS accounting, specify a number from 1 to 10. The default value in the Ethernet profile is 0 (zero). The default in a Connection profile is 1.

When setting the timer for RADIUS/LOGOUT authentication, specify a number between 0 and 655353. The default is 0, which means that no Session Events are sent.

Example: `Sess Timer=10`

Dependencies: For accounting, this parameter applies only to RADIUS—because the Terminal Access Concentrator Access Control Server Plus (TACACS+) uses TCP, it has its own timeout method. For authentication, this parameter applies only to RADIUS/LOGOUT.

Location: Ethernet > Mod Config > Accounting, Ethernet > Mod Config > Auth

See Also: Acct, Auth

Shared Prof

Description: Specifies whether multiple users can share a single Connection profile or a single RADIUS user profile *or* whether a single user can have multiple sessions active.

Sharing a profile cannot result in two IP addresses sharing the same interface. As a result, this parameter is typically used to share profiles when the caller is assigned an IP address dynamically, which ensures that each caller is assigned a unique address.

Usage: Specify Yes or No.

- Yes means the DSL Terminator unit allows more than one caller to share the same profile, provided that no IP address conflicts will result.
- No means the DSL Terminator unit does not allow shared profiles. No is the default.

Example: `Shared Prof=Yes`

Dependencies: This parameter does not apply to connections that have hard-coded IP addresses. For the Ascend-Shared-Profile-Enable attribute to apply, you must disable shared profiles for the DSL Terminator unit as a whole with Ethernet > Mod Config > Shared Prof = No.

Location: Ethernet > Mod Config, Ethernet > Connections

Single Answer

Description: Specifies whether the DSL Terminator completes the answering and routing of one call before answering and routing the next call.

Usage: Specify Yes or No.

- Yes means the DSL Terminator will answer and route one call before answering and routing the next call. Yes is the default, and should be used if the DSL Terminator is not configured for dual-port calls, or if an incoming call is explicitly routed. Yes is the default.
- No means the DSL Terminator will answer and route an incoming call immediately.

Example: `Single Answer=No`

Location: System > Sys Config

See Also: Ans #, B1 Prt/Grp, B2 Prt/Grp, Ch *N* Prt/Grp

SNMP Authentication

Description: Specifies whether the DSL Terminator unit traps security events and sends a traps PDU to the SNMP manager. Security events notify users of security problems and track access to the unit. The DSL Terminator unit traps the following security events:

Event	Indication
authenticationFailure (RFC-1215 trap-type 4)	The DSL Terminator unit sending the trap is the addressee of a protocol message that is not properly authenticated.
consoleStateChange (Lucent trap-type 12)	The console associated with the passed console index has changed state.
maxTelnetAttempts (Lucent trap-type 15)	There have been three consecutive failed attempts to log into the DSL Terminator unit via Telnet.

Usage: Specify Yes or No.

- Yes specifies that the DSL Terminator unit sends security-event traps to the host specified by Host-Address. The default is Yes.
- No specifies that the DSL Terminator unit does not send security-event traps.

Example: `SNMP Authentication=No`

Location: Ethernet > SNMP Traps > Enable Traps

SNTP Enabled

Description: Specifies whether the DSL Terminator unit uses SNTP (Simple Network Time Protocol—RFC 1305) to set and maintain its system time by communicating with an SNTP server. SNTP must be enabled for the DSL Terminator unit to communicate using that protocol. When enabled, the DSL Terminator unit polls the SNTP server every 50 seconds.

Usage: Specify one of the following values:

- Enabled specifies that the DSL Terminator unit uses an SNTP server to maintain its time.
- Disabled specifies that the DSL Terminator unit does not use an SNTP server.
- Passive specifies that the DSL Terminator unit takes appropriate action if it finds a difference between the SNTP server and the system clock.

Example: `SNTP Enabled=Disabled`

Dependencies: Consider the following:

- If you enable SNTP, you must specify at least one SNTP server address.
- If you set SNTP Enabled=Passive, and the DSL Terminator unit determines that the difference between the SNTP time and the system clock is larger than the value of SNTP Threshold, the DSL Terminator unit does not apply the time difference to the system clock. Instead, the DSL Terminator unit sends out an SNMP trap once every 24 hours.
- If you set SNTP Enabled=Passive, and the DSL Terminator unit receives an SNTP update showing that the difference between the SNTP time and the system clock is lower than or

equal to the value of SNTP threshold, the DSL Terminator unit records the clock difference, discards the update (and any subsequent updates), and sends out an SNMP trap to report that the system can no longer correct its time. The system then applies the clock difference when you reset the unit.

Location: Ethernet > Mod Config > SNTP Server

See Also: SNTP Host #N, Time Zone

SNTP Host #N (N=1–3)

Description: Specifies the IP address of up to three SNTP servers. The DSL Terminator unit polls the SNTP Host every 50 seconds. If the server specified by SNTP Host #1 is not active, the DSL Terminator unit sends its requests to SNTP Host #2. If that server is not active, the DSL Terminator unit sends its requests to SNTP Host #3.

Usage: Specify an IP address. The default is 0.0.0.0.

Example: `SNTP Host #1=10.3.3.100`

Dependencies: This parameter does not apply if SNTP is not enabled.

Location: Ethernet > Mod Config > SNTP Server

See Also: SNTP Enabled, Time Zone

SNTP Threshold

Description: Specifies the maximum time difference (in seconds) between the SNTP server and system clock that the DSL Terminator unit can correct without a system reset.

Usage: Specify an integer. The default is 10.

Example: `SNTP Threshold=9`

Dependencies: You must set SNTP Enabled=Passive for SNTP Threshold to apply.

Location: Ethernet > Mod Config > SNTP Server

See Also: SNTP Enabled

Source Addr

Description: Specifies an IP address. If specified, the DSL Terminator unit ignores packets from that source for monitoring purposes. If a Source Mask is also specified, the DSL Terminator unit uses the combined address and mask to ignore packets from the specified source.

Note: Heartbeat monitoring is optional. It is not required for multicast forwarding.

Usage: Specify an IP address.

Dependencies: To set up heartbeat monitoring, you must configure several parameters that define what packets will be monitored, how often and how long to poll for multicast packets,

and the threshold for generating an alarm. These parameters do not apply if multicast forwarding is not in use.

Location: Ethernet > Mod Config > Multicast

See Also: Alarm Threshold, HeartBeat Addr, HeartBeat Slot Count, HeartBeat Slot Time, Heartbeat Udp Port, Source Mask,

SourceIP Check

Description: Enables or disables antispoofing for the session.

Usage: Specify Yes or No.

- Yes specifies that the system checks all packets received on the interface The source IP address in each packet must match the far end remote address or the address agreed upon in Internet Protocol Control Protocol (IPCP) negotiation. If the addresses do not match, the system discards the packet.
- No disables antispoofing for the session. The default is No.

Example: `SourceIP Check=Yes`

Location: Ethernet > Connections > IP Options

Source Mask

Description: Specifies an IP netmask. If specified, the DSL Terminator unit uses the combined address and mask to ignore packets from the specified source for heartbeat monitoring purposes.

Note: Heartbeat monitoring is optional. It is not required for multicast forwarding.

Usage: Specify a netmask.

Example: `Source Mask=255.255.255.248`

Dependencies: To set up heartbeat monitoring, you must configure several parameters that define what packets will be monitored, how often and for how long to poll for multicast packets, and the threshold for generating an alarm. These parameters do not apply if multicast forwarding is not in use.

Location: Ethernet > Mod Config > Multicast

See Also: HeartBeat Addr, Heartbeat Udp Port, Source Addr, HeartBeat Slot Time, HeartBeat Slot Count, Alarm Threshold

Split Code.User

Description: Divides the PIN and CODE of a user and their USERNAME by a period. If the CHAP field cannot accommodate the full PIN+CODE.USER, you can enable this feature. The DSL Terminator unit splits the passcode into two pieces with the information following the period becoming the CHAP Name, overriding the name of the router.

Usage: Specify one of the following values:

- Yes—Enables PIN, CODE and USERNAME to be divided.
- No— Disables this feature. No is the default.

Example: `Split Code.User=No`

Location: Ethernet > Connections > Encaps Options

Src Adrs

Description: Specifies a source IP address. After this value has been modified by applying the specified Src Mask, it is compared to a packet's source address.

Usage: Specify a source IP address that the DSL Terminator unit uses for comparison when filtering a packet. The zero address 0.0.0.0 is the default. If you accept the default, the DSL Terminator unit does not use the source address as a filtering criterion.

Example: Src Adrs=10.62.201.56

Dependencies: This parameter applies only to filters of type IP.

Location: Ethernet > Filters > Input filters > In filter *N* > IP, Ethernet > Filters > Output filters > Out filter *N* > IP, Ethernet > Filters > Input filters > In filter *N* > IPTOS, Ethernet > Filters > Output filters > Out filter *N* > IPTOS

See Also: Src Mask

Src Mask

Description: Specifies a mask to apply to the Src Adrs value before comparing it to the source address in a packet. You can use it to mask out the host portion of an address, for example, or the host and subnet portion.

The DSL Terminator unit applies the mask to the address using a logical AND after the mask and address are both translated into binary format. The mask hides the portion of the address that appears behind each binary 0 (zero) in the mask. A mask of all zeros (the default) masks all bits, so all source addresses are matched. A mask of all ones (255.255.255.255) masks no bits, so the full source address to a single host is matched.

Usage: Specify the mask in dotted decimal format. The zero mask 0.0.0.0 is the default; this setting indicates that the DSL Terminator unit masks all bits. To specify a single source address, set Src Mask=255.255.255.255 and set Src Adrs to the IP address that the DSL Terminator unit uses for comparison.

Example: `Src Mask=255.255.255.0`

Dependencies: This parameter applies only to filters of type IP.

Location: Ethernet > Filters > Input filters > In filter *N* > IP, Ethernet > Filters > Output filters > Out filter *N* > IP, Ethernet > Filters > Input filters > In filter *N* > IPTOS, Ethernet > Filters > Output filters > Out filter *N* > IPTOS

See Also: Src Adrs

Src Port

Description: Specifies a value to compare with the source port number in a packet. The default setting (zero) indicates that the DSL Terminator unit disregards the source port in this filter. Port 25 is reserved for SMTP; that socket is dedicated to receiving mail messages. Port 20 is reserved for FTP data messages, port 21 for FTP control sessions, and port 23 for Telnet.

Note: The Src Port Cmp parameter specifies the type of comparison to be made.

Usage: Specify a number between 0 and 65535.

Example: `Src Port #=25`

Dependencies: This parameter applies only to filters of type IP.

Location: Ethernet > Filters > Input filters > In filter *N* > IP, Ethernet > Filters > Output filters > Out filter *N* > IP, Ethernet > Filters > Input filters > In filter *N* > IPTOS, Ethernet > Filters > Output filters > Out filter *N* > IPTOS

See Also: Dst Port #, Dst Port Cmp, Src Port Cmp

Src Port Cmp

Description: Specifies the type of comparison the DSL Terminator unit makes when filtering for source port numbers using the Src Port # parameter.

Usage: Specify one of the following values:

- None (the default) means the DSL Terminator unit does not compare source port numbers.
- Less means the comparison succeeds if the number is less than the value of Src Port #.
- Eql means the comparison succeeds if the number equals the value of Src Port #.
- Gtr means the comparison succeeds if the number is greater than the value of Src Port #.
- Neq means the comparison succeeds if the number is not equal to the value of Src Port #.

Example: `Src Port Cmp=None`

Location: Ethernet > Filters > Input filters > In filter *N* > IP, Ethernet > Filters > Output filters > Out filter *N* > IP, Ethernet > Filters > Input filters > In filter *N* > IPTOS, Ethernet > Filters > Output filters > Out filter *N* > IPTOS

See Also: Src Port #

Static Preference

Description: Specifies the default preference value for statically configured routes.

Usage: Specify a number between 0 and 255. The default value is 100. Zero is the default for connected routes (such as the Ethernet). The value of 255 means *Don't use this route*.

Example: `Static Preference=100`

Dependencies: These are the default route preference values:

- Routes learned from OSPF=10

- Routes learned from ICMP Redirects=30
- Routes learned from RIP=100
- Static routes in an IP Route profile or Connection profile=100

Location: Ethernet > Mod Config > Route Pref

Station

Description: Specifies the name of the far end device in this Connection profile.

Note: If this Connection profile specifies a nailed link to the Home Network for a DSL Terminator unit acting as an ATMP Home Agent in gateway mode, the Station name must match the Ascend-Home-Network-Name attribute in the Foreign Agent's RADIUS configuration.

Usage: Specify the name of the far end device. You can enter up to 31 characters. Make sure you specify the name exactly, including case changes.

Example: `Station=NewYork`

Location: Ethernet > Connections

See Also: ATMP Mode, Type

Status N (N=1–8)

Description: Enables you to customize the status windows in the VT100 interface so that particular screens appear at startup. The numbers 1 through 8 indicate the position of the status window, starting with the upper left. You can also use Ctrl-D-M to automatically configure the Status parameter.

Usage: Specify a window number in the format *XY-NNN*.

- *X* is the module number, and indicates a virtual or real module.
- *Y* is the port number.
- The three digits after the dash are the root number.

  A root number of 000 identifies a top-level branch of the tree. If *N* is not 0 (zero), the root number identifies a window lower in the tree.

Example: `Status 1=20-100`

Location: System > Sys Config

See Also: Ethernet, Connection

Sub-Adr

Description: Specifies how the DSL Terminator treats incoming calls based on whether they convey an ISDN subaddress.

Usage: Specify one of the following values:

- Termsel specifies that the DSL Terminator must use an ISDN subaddress to determine whether a call is answered.

  The called-party number must have a subaddress that matches a subaddress in the Line profile of the line on which the DSL Terminator receives the call. Otherwise, the DSL Terminator ignores the call. If the DSL Terminator accepts the call, the subaddress becomes part of the incoming phone number, and the DSL Terminator uses it in Ans # comparisons.

  This setting is intended for a scenario in which equipment is connected to a multidrop ISDN BRI line.
- Routing specifies that the called-party number may or may not have a subaddress.

  If a subaddress is present, it becomes part of the incoming phone number. The DSL Terminator matches it against the value of the Serial, LAN, DM, and V.110 parameters in the Sys Config menu in order to determine the interface to which it should route the call. If no match is found, the DSL Terminator uses the subaddress in Ans # comparisons.
- None specifies that the DSL Terminator does not use subaddressing.

Example: `Sub-Adr=Routing`

Location: System > Sys Config

See Also: Ans #, DM, LAN, Serial, V.110

Sub Pers

Description: Specifies a n umber of seconds for which the ALU (average link utilization) must persist below the Target Util threshold before the DSL Terminator subtracts bandwidth. When utilization falls below the threshold for a period of time greater than the value of the Sub Pers parameter, the DSL Terminator attempts to remove the number of channels specified by the Dec Ch Count parameter. However, the DSL Terminator never subtracts enough bandwidth to clear the call or cause the channel count to fall below the specified minimum. Setting the Add Pers and Sub Pers parameters prevents the system from continually adding and subtracting bandwidth, and can slow down the process of allocating or removing bandwidth. Add Pers and Sub Pers have little or no effect on a system with a high Sec History value. However, if the value of Sec History is low, the Add Pers and Sub Pers parameters provide an alternative way to ensure that spikes persist for a certain period of time before the system responds.

Usage: Usage: Specify a number between 1 and 300. When the DSL Terminator is using MP+, the default value is 10. When the DSL Terminator is using dynamic AIM, the default value is 20.

Example: `Sub Pers=15`

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options

See Also: Add Pers, Dec Ch Count, Dyn Alg, Min Ch Count, Sec History, Target Util

Suppress Host Routes

Description: Specifies whether the DSL Terminator unit advertises host routes in each update, which can cause excessive routing overhead:

Usage: Specify Yes or No.

- Yes specifies that host routes are suppressed,
- No specifies that host routes are advertised. The default is No.

Example: `Suppress Host Routes=Yes`

Dependencies: If you set Suppress Host Routes to Yes, routes are suppressed according to the following rules:

- If a Connection profile specifies a LAN Adrs setting with a subnet mask of less than 32 bits, host routes for the interface are suppressed while the session is being negotiated. After the session is established, only network routes are advertised for the interface.
- If a Connection profile specifies a LAN Adrs setting with a subnet mask of /32, host routes for the interface are not suppressed.

Location: Ethernet > Mod Config

See Also: LAN Adrs

Sys Diag

Description: Enables or disables permission to perform all system diagnostics.

Usage: Specify Yes or No.

- Yes means the operator can use the commands in the Sys Diag menu. Yes is the default.
- No specifies that an operator cannot use any of those commands.

Example: `Sys Diag=No`

Location: System > Security

Syslog

Description: Specifies whether the DSL Terminator unit sends warning, notice, and Call Detail Reporting (CDR) records from the system logs to the Syslog host.

Usage: Specify Yes or No.

- Yes enables the DSL Terminator unit to communicate with the Syslog host.
- No disables this function. No is the default.

Example: `Syslog=No`

Dependencies: If you enable Syslog, you must enter the IP address of the Syslog host in the Log Host parameter.

Location: Ethernet > Mod Config

See Also: Log Facility, Log Host

T

T391

Description: Specifies the number of seconds between Status Enquiry messages.

Usage: Specify a number between 5 and 30. The default is 10.

Example: `T391=25`

Dependencies: This parameter applies only if Link Mgmt=T1.617D and T392 is set to a nonzero value.

Location: Ethernet > Frame Relay

See Also: Link Mgmt, T392

T392

Description: Specifies the number of seconds the DSL Terminator unit waits for a Status Enquiry message before recording an error. If you specify zero, the DSL Terminator unit does not process WAN-side Status Enquiry messages. If you specify a nonzero value, the DSL Terminator unit uses T1.617D (a link management protocol defined in ANSI T1.617 Annex D) to monitor another DSL Terminator unit over a nailed-up connection.

Usage: Specify 0 (zero), or a number between 5 and 30. The default is 15.

Example: `T392=25`

Dependencies: The T392 parameter applies only if Link Mgmt=T1.617D.

Location: Ethernet > Frame Relay

See Also: Link Mgmt T391

Target Util

Description: Specifies a percentage of line utilization to use as a threshold for determining when to add or subtract bandwidth. When the value is 70%, the device adds bandwidth when it exceeds a 70 percent utilization rate, and subtracts bandwidth when it falls below that number.

Usage: Specify a number between 0 and 100. The default is 70 (70% utilization).

Example: Target Util=70

Dependencies: In a Call profile, this parameter applies only to dynamic AIM calls. It specifies the target percentage of bandwidth utilization for a dynamic time period.

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options

See Also: See Also: Add Pers, Call Mgm, Call Type, Dec Ch Count, Dyn Alg, Inc Ch Count, Sec History, Sub Pers

Term Rate

Description: Specifies the bit rate of a serial port. When you modify the bit rate of a serial port, you might also need to change the data rate setting of the terminal accessing that port.

Usage: Specify one of the following values:

- 57600
- 38400
- 19200
- 9600 (the default)
- 4800
- 2400

Example: `Term Rate=9600`

Location: System > Sys Config

Time

Description: Specifies the time of day.

Usage: Specify the time of day in the format *hour :minutes :seconds*. The default is 00:00:00.

Example: `Time=13:24:24`

Location: System > Sys Config

Time Zone

Description: Specifies your time zone as an offset from the Universal Time Configuration (UTC) to enable the DSL Terminator unit to update its system time from an SNTP server. UTC is in the same time zone as Greenwich Mean Time (GMT), and the offset is specified in hours using a 24-hour clock. Because some time zones, such as Newfoundland, cannot use an even hour boundary, the offset includes four digits and is stated in half-hour increments. For example, in Newfoundland the time is 1.5 hours ahead of UTC, which is represented as follows:

```
UTC+0130
```

For San Francisco, which is 8 hours ahead of UTC, the time is represented as follows:

```
UTC+0800
```

For Frankfurt, which is 1 hour behind UTC, the time is represented as follows:

```
UTC-0100
```

Usage: Specify one of the following values to represent your time zone:

```
utc-1130
utc-1100
utc-1030
utc-1000
utc-0930
utc-0900
```

```
utc-0830
utc-0800
utc-0730
utc-0700
utc-0630
utc-0600
utc-0530
utc-0500
utc-0430
utc-0400
utc-0330
utc-0300
utc-0230
utc-0200
utc-0130
utc-0100
utc-0030
utc+0000
utc+0030
utc+0100
utc+0130
utc+0200
utc+0230
utc+0300
utc+0330
utc+0400
utc+0430
utc+0500
utc+0530
utc+0600
utc+0630
utc+0700
utc+0730
utc+0800
utc+0830
utc+0900
utc+0930
utc+1000
utc+1030
utc+1100
utc+1130
utc+1200
```

Example: `Time zone=UTC -0700`

Dependencies: This parameter is not applicable unless SNTP Enabled is set to Yes.

Location: Ethernet > Mod Config > SNTP Server

See Also: SNTP Enabled, SNTP Host #

TOS

Description: Specifies the type of service for the data stream.

Usage: The three most significant bits of the Type-of-Service (TOS) byte are priority bits used to set precedence for priority queuing. The next four bits of the TOS byte are used to choose a link based on the type of service. When TOS is enabled, you can set one of the following values in the packet:

- Normal specifies normal service (the default).
- Cost minimizes monetary cost.
- Reliability maximizes reliability.
- Throughput maximizes throughput.
- Latency minimizes delay.

Example: `TOS=Cost`

Location: Ethernet > Connections > IP Options

See Also: Active, Apply To, Precedence

TOS Enabled

Description: Enables or disables Type of Service (TOS) for the connection.

Usage: Specify Yes or No.

- Yes enables TOS for the connection.
- No disables TOS for the connection. The default is No.

Example: `TOS Enabled=Yes`

Location: Ethernet > Connections > IP Options

See Also: TOS, TOS Filter

TOS Filter

Description: Specifies the name of a Filter profile that defines a Type-of-Service (TOS) filter.

Usage: Specify the name of a defined profile. The default is null.

Example: `TOS Filter=filtertos`

Location: Ethernet > Connections > IP Options

See Also: TOS, TOS Enabled

Traffic Shaper

Description: Specifies the Traffic Shaper Profile to be used for a Virtual channel (VC) connection. Note that the Aggregate parameter determines the throughput for each VC that shares a traffic shaper. By default, each VC using a traffic shaper attempts to use the entire bandwidth allocated for the shaper.

Usage: Specify a number between 1 and 16. The default is 16. Traffic Shapers profiles 1 through 15 are configured in the Net/DS3-ATM profile, the Net/OC3-SMF-ATM profile, or the

Net/OC3-UTP-ATM profile. Traffic Shaper profile 16 is the system default. For information on the default Traffic Shaper profile, see the DSL Terminator *Network Configuration Guide*.

Example: `Traffic Shaper=8`

Dependencies: You must re-establish the session for changes to the Traffic Shaper parameter to take effect.

Location: Net/DS3-ATM > Line Config > *any line profile* > Traffic Shapers, Net/OC3-SMF-ATM > Line Config > *any line profile* > Traffic Shapers, Net/OC3-UTP-ATM > Line Config > *any line profile* > Traffic Shapers

See Also: Aggregate, Bit Rate, Enabled, Max Burst Size, Peak Rate, Priority

Transit

Description: Specifies a string for use in the *transit network IE* for PRI calling when going through an Interexchange Carrier (IEC). The default (null) causes the DSL Terminator to use any available IEC for long-distance calls.

Usage: Specify one of the following dialing prefixes:

- 288 (AT&T)
- 222 (MCI)
- 333 (Sprint)

Example: `Transit #=222`

Dependencies: The Transit # value in the Dial Plan profile overrides the Transit # value in the Call profile or the Connection profile. This parameter does not apply to nailed connections.

Location: Host/Dual (Host/AIM6) > Port*N* Menu > Directory, Ethernet > Connections > Telco Options, Ethernet > Frame Relay, System > Dial Plan, Ethernet > X.25

See Also: B1 Trnk Grp, B2 Trnk Grp, Ch *N* Trnk Grp

TrnkGrp

Description: Specifies a trunk group number, assigning a channel to a trunk group.

Usage: Specify a trunk group number from 2 to 9. The default is 9.

Example: `TrnkGrp=5`

Location: Net/ATM-DS3 > Line Config, Net/UDS3 > Line Config, Net/SDSL-8 > Line Config > Line *N*, Net/SDSL-16 > Line Config > Line *N*

See Also: Activation, Line Rate, Nailed-Group,

TX-Data-Rate-Limit

Description: Specifies the maximum data rate (in k-bits per second) to be transmitted across the connection. You can use this setting to limit bandwidth for a connection according to the rate charged for the account.

Usage: Specify a number from 0 to 64000. The default is 0 (zero), which disables the data-rate limit feature. If the value you specify is larger than the actual bandwidth provided by the line, the connection behaves as though the data rate limit were disabled, except that additional computations are performed unnecessarily.

Example: `set tx-data-rate-limit=32000`

Dependencies: The system activates configurable transmit data-rate limits only for connections that use CAP-RADSL, SDSL, and unchannelized DS3 cards. If you specify a value for a connection that does not use these cards, the system ignores the settings.

Location: Connection > Session-Options

See Also: R/W Comm

Type

Description: Specifies the type of ATMP functionality supported in the DSL Terminator unit, or if it appears in a filter, the action performed by the filter.

Usage: Specify one of the following values:

In an Ethernet profile:

- Router specifies that the DSL Terminator unit is an ATMP Home Agent in routing mode (the default for ATMP Home Agents)
- Gateway specifies that the DSL Terminator unit is an ATMP Home Agent in gateway mode.

In a Filter profile:

- Generic means the filter examines byte and offset values within packets, regardless of which protocol is in use (the default in Filter profiles).
- IP means the filter examines the IP-specific fields within packets.

Example: `NumPlanID=ISDN`

Location: Ethernet > Mod Config > ATMP Options, Ethernet > Filters > Input filters > In filter N, Ethernet > Filters > Output filters > Out filter N

See Also: ATMP Gateway, ATMP Mode, Password, Station, UDP Port, Valid

Type of Service

Description: Specifies the type of service for the data stream.

Usage: The three most significant bits of the Type-of-Service (TOS) byte are priority bits used to set precedence for priority queuing. The next four bits of the TOS byte are used to choose a link based on the type of service. When TOS is enabled, you can set one of the following values in the packet:

- Normal specifies normal service (the default).
- Cost minimizes monetary cost.
- Reliability maximizes reliability.
- Throughput maximizes throughput.
- Latency minimizes delay.

Example: `Type of Service=Cost`

Location: Ethernet > Filters > Input filters > In filter *N* > IPTOS, Ethernet > Filters > Output filters > Out filter *N* > IPTOS

U

UDP Cksum

Description: Enables or disables the use of UDP checksums on this interface. If enabled, the DSL Terminator unit generates a checksum whenever it sends out a UDP packet. It sends out UDP packets for queries and responses related to the following protocols:

- ATMP
- SYSLOG
- DNS
- ECHOSERV
- RADIUS
- TACACS
- RIP
- SNTP
- TFTP

Note: You might want to enable this parameter if data integrity is of the highest concern for your environment, and having redundant checks is important. This setting is also appropriate if your UDP-based servers are located on the remote side of a WAN link that is prone to errors.

Usage: Specify Yes or No.

- Yes generates UDP checksums for queries and responses related to protocols that use UDP.
- No disables UDP checksums. No is the default.

Example: `UDP Cksum=Yes`

Location: Ethernet > Mod Config

UDP Port

Description: Specifies a UDP port number on which the DSL Terminator unit listens when using ATMP.

Note: Units that use UDP to communicate for a particular purpose must all agree on the assigned port number.

Usage: Specify a valid UDP port number (0–65535). The default port number is 5150.

Example: `UDP Port=5150`

Dependencies: This parameter must match the UDP port configured in other units that communicate with the DSL Terminator unit for the specified function. ATMP uses UDP port 5150 for ATMP messages between the Foreign and Home Agents. If you specify a different UDP port number, make sure that the entire ATMP configuration agrees.

Note: A system reset is required for the ATMP subsystem to recognize the new UDP port number.

Location: Ethernet > Mod Config > ATMP Options

See Also: ATMP Gateway, ATMP Mode, Password, Type

Example: `Unit Type=CPE`

Upload

Description: Enables or disables permission to upload the DSL Terminator unit's configuration from another device.

Usage: Specify Yes or No.

- Yes means the operator can upload the DSL Terminator unit's configuration from another device. This setting has the potential of clearing all passwords in the DSL Terminator unit. Yes is the default.
- No disables this permission.

Example: `Upload=No`

Dependencies: This parameter is not applicable if the Operations permission is disabled.

Location: System > Security

Use Answer as Default

Description: Indicates whether the Answer profile should override the factory default Internet profile when the DSL Terminator unit validates an incoming call using RADIUS or TACACS.

Usage: Specify Yes or No.

- Yes instructs the DSL Terminator unit to use the Answer profile for default values.

  When set to Yes, the DSL Terminator unit falls back to the value specified in the Answer profile for options that are not specified in a given external authentication profile. This setting does not affect Connection profiles in any way.
- No means the DSL Terminator unit uses the factory default Internet profile instead.

  When set to No, the DSL Terminator unit uses factory defaults for options not specified in a external authentication profile, rather than the values set in the Answer profile. No is the default.

Example: `Use Answer as Default=Yes`

Location: Ethernet > Answer

Use Exceeded

Description: Specifies whether the system generates a trap when a specific port has exceeded the number of DS0 minutes allocated to it or the system DS0 usage has been exceeded.

Usage: Specify Yes or No.

- Yes specifies that the system generates a trap when a specific port has exceeded the number of DS0 minutes allocated to it or the system DS0 usage has been exceeded. The default is Yes.
- No specifies that the system does not generate a trap when a specific port has exceeded the number of DS0 minutes allocated to it or the system DS0 usage has been exceeded.

Example: `Use Exceeded=No`

Location: Ethernet > SNMP Traps > Enable Traps

Use TACACS+

Description: Specifies whether the DSL Terminator unit uses a TACACS+ server to authenticate the user specified by the Security profile.

Usage: Specify Yes or No.

- Yes specifies that the user is authenticated by a TACACS+ server.
- No specifies that the user is not authenticated by a TACACS+ server.The default is No.

Example: `Use TACACS+=Yes`

Dependencies: For Use TACACS+ to apply, you must set Auth=TACACS+.

Location: System > Security

See Also: Auth

Use Trunk Grps

Description: Specifies the use of trunk groups for all network lines. When trunk groups are in use, channels must be assigned trunk group numbers to be available for outbound calls.

Usage: Specify Yes or No.

- Yes means all channels must be assigned a trunk group number to be available for outbound calls.
- No means trunk groups are not used. No is the default.

Example: `Use Trunk Grps=Yes`

Dependencies: When this parameter is set to Yes, channel configurations must specify trunk-group assignments.

Location: System > Sys Config

See Also: Call Type, Dial #

V

Valid

Description: In a Filter profile, enables or disables the current input or output filter. In a Static Mapping *N* submenu, enables or disables the routing of incoming packets for a particular TCP or UDP port to a specific server and port on the local network.

Note: If you change the value of Profile in a Static Mapping *N* submenu, the change does not take effect until the next time a connection is made to the remote network. To make the change immediately, you must terminate the connection to the remote network and then reopen it.

Usage: Specify Yes or No.

In a Filter profile:

- Yes activates the filter and enables its configuration.
- No disables the filter, causing the DSL Terminator unit to skip it when filtering the data stream. No is the default.

In a Static Mapping *N* submenu:

- Yes enables the routing of incoming packets specified by the other parameters in the same Static Mapping *N* submenu.
- No disables the routing of incoming packets specified by the other parameters in the same Static Mapping *N* submenu.

Example: `Valid=Yes`

Location: Ethernet > Filters > Input filters > In filter *N*, Ethernet > Filters > Output filters > Out filter *N*

See Also: Type

Value

Description: Specifies a hexadecimal number to be compared to specific bits contained in packets after the Offset, Length, and Mask calculations have been performed. The DSL Terminator unit compares only the unmasked portion of a packet to the Value parameter. The length of the Value parameter must contain the number of bytes specified by the Length parameter.

Usage: Specify a hexadecimal number up to 12 bytes.

Example: `Value=e0e0030000000000`

Location: Ethernet > Filters > Input filters > In filter *N* > Generic, Ethernet > Filters > Output filters > Out filter *N* > Generic

See Also: Length, Mask, Offset

Version

Description: Specifies the version number of a Secure Access Firewall. Each firewall contains a version number to ensure that any firewall that is uploaded to the router is

compatible with the firewall software on the DSL Terminator unit. Secure Access Manager (SAM) checks the version number before uploading a firewall.

Usage: This parameter cannot be edited.

Example: Version=14.02

Location: Ethernet > Firewalls

Virtual Router

Description: Specifies the name of the Virtual Router (VRouter) for which the DSL Terminator unit creates a static route.

Usage: Specify the name of a Virtual Router. The default is null, which specifies that the unit uses the global Virtual Router (Main).

Example: `Virtual Router=SL2`

Dependencies: The Virtual Router parameter is valid only if the Sys Option Status display specifies VRouter Avail.

Location: Ethernet > Static Rtes > *any Static Rtes profile*, Ethernet > Connections> *any Connection profile*>IP Options

See Also: Active, Allow As Client DNS, Dest VRouter, Domain Name, Name, Pool*#N* Count, Pool*#N* Name, Pool*#N* Start, Pool Summary, Pri DNS, RIP Policy, RIP Summary, RIP Trigger, Sec DNS, Sec Domain Name, VRouter IP Adrs

VJ Comp

Description: Specifies whether Van Jacobson IP header compression is negotiated on incoming calls using encapsulation protocols that support this feature. VJ Comp applies only to packets in TCP applications, such as Telnet. Turning on header compression is most effective in reducing overhead when the data portion of the packet is small.

Usage: Specify Yes or No.

- Yes enables VJ compression for TCP packets.
  This is the default.
- No disables VJ compression. No is the default.

Example: `VJ Comp=Yes`

Location: Ethernet > Answer > PPP Options, Ethernet > Connections > Encaps Options

VPI/VCI Range

Description: Specifies a VPI-VCI range.

Usage: Specify one of the following ranges:

0–1/32–32768
0–3/32–16383

0–7/32–8191
0–15/32–4095 (the default)
0–31/32–2047
0–63/32–1023
0–127/32–511
0–255/32–255

Example: `VPI/VCI Range=0-1/32-32768`

Location: Net/ATM-DS3 > Line Config > Line *N*

VRouter IP Adrs

Description: When the DSL Terminator unit supports a Virtual Router (VRouter) domain, VRouter IP Adrs specifies the default local IP address the unit uses for any outgoing packets generated by the VRouter.

Usage: Specify an IP address in dotted decimal notation. The default is 0.0.0.0.

Example: `VRouter IP Adrs=0.0.0.0`

Dependencies: The VRouter IP Adrs parameter is valid only if the Sys Option Status display specifies VRouter Avail.

Location: Ethernet > Virtual Routers > *any Virtual Routers profile*

See Also: Active, Allow As Client DNS, Dest VRouter, Domain Name, Pool#N Count, Pool#N Name, Pool#N Start, Pool Summary, Pri DNS, RIP Policy, RIP Summary, RIP Trigger, Sec DNS, Sec Domain Name, Virtual Router

W

WAN Alias

Description: Specifies the IP address of the link's remote interface to the WAN. It is used to identify a numbered interface at the remote end of the link. If an address is specified for WAN alias, the following events occur:

- Host routes are created both to the Lan Adrs and the WAN Alias address. The WAN Alias will be listed in the routing table as a gateway (next hop) to the Lan Adrs.
- A route is created to the remote system's subnet, showing the WAN Alias as the next hop.
- Incoming PPP/MP+ calls must report their IP addresses as the WAN Alias (rather than the Lan Adrs). That is, the caller must be using a numbered interface, and its interface address must agree with the WAN Alias on the receiving side.

If you want to create static routes to hosts at the remote end, you can use the WAN Alias address as the "next hop" (gateway) field. (The Lan Adrs address will also work, as would be used for system-based routing.)

Usage: Specify the IP address of the remote interface. The default is 0.0.0.0/0.

Example: `WAN Alias=10.207.23.7/24`

Dependencies: This parameter does not apply if the connection does not route IP.

Location: Ethernet > Connections > IP Options

See Also: Route IP, IF Adrs

Warm Start

Description: Specifies whether the system generates a trap when the DSL Terminator unit reinitializes itself so that neither the configuration of the SNMP manager nor of the system itself is altered.

Usage: Specify Yes or No.

- Yes specifies that the system generates a trap when the DSL Terminator unit reinitializes itself so that neither the configuration of the SNMP manager nor of the system itself is altered. The default is Yes.
- No specifies that the system does not generates a trap when the DSL Terminator unit reinitializes itself so that neither the configuration of the SNMP manager nor of the system itself is altered.

Example: `Warm Start=No`

Location: Ethernet > SNMP Traps > Enable Traps

See Also: Cold Start

Z

Zone Name #N

Description: Specifies the name of the AppleTalk zone to which the DSL Terminator unit is connected. If the local Ethernet network supports an AppleTalk router with configured zones, you can place the DSL Terminator unit in one of those zones.

A zone is a multicast address containing an arbitrary subset of the AppleTalk nodes in an internet. Each node belongs to only one zone, but a particular extended network can contain nodes belonging to any number of zones. Zones provide departmental or other groupings of network entities that a user can easily understand. If the DSL Terminator unit is an AppleTalk router, it brings up the line when it receives packets addressed to the network number (defined by Net Start and Net End) or zone name specified for the remote connection, and routes packets to the appropriate network or zone.

Usage: Specify the name of a zone that has been configured on the local Ethernet network. Enter up to 33 alphanumeric characters.

If you do not specify a name and AppleTalk=Yes, the DSL Terminator unit acquires its zone(s) from the seed router on the network, including the default zone.

In an Ascend AppleTalk router, zone names are not case sensitive. However, some routers regard zone names as case sensitive, and you should be consistent in spelling zone names when you configure multiple connections or routers. Although AppleTalk permits the use of spaces in zone names, it does not consider an underscore to be the same as a space. Since some routers do equate the underscore and the space, or do not recognize a space as a valid character, it is advisable to use only the underscore in a network with routers other than Ascend routers.

Example:
```
Default Zone=SALES
Zone Name #1=MKTG
Zone Name #2=ENGINEERING
Zone Name #3=ADMIN
 Zone Name #4=BRANCH
```

Dependencies: If AppleTalk is disabled, the Zone Name parameter does not apply.

Location: Ethernet > Mod Config > AppleTalk

See Also: Default Zone, Net Start, Net End, AppleTalk Router

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z