Lucent Technologies
Bell Labs Innovations

DSL Terminator™

Network Configuration Guide

Part Number: 7820-0772-001
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

Customer Service iii

About This Guide xvii

What is in this guide xvii
What you should know xvii
Documentation conventions xviii
Related publications xix

Chapter 1 Getting Acquainted with the DSL Terminator 1-1

Overview of DSL Terminator configuration 1-1
- Creating a network diagram 1-1
- Configuring lines, slots, and ports for WAN access 1-1
- Configuring WAN connections and security 1-1
- Concentrating Frame Relay connections 1-2
- Configuring routing and bridging across the WAN 1-2
  - Enabling protocol-independent packet bridging 1-2
  - IP routing 1-2
- Configuring Internet services 1-2

Management features 1-3
- Using the terminal-server command line 1-3
- Using status windows to track WAN or Ethernet activity 1-3
- Using SNMP to manage the unit 1-3
- Using remote management to configure far-end units 1-3
- Flash RAM and software updates 1-4
- Call Detail Reporting (CDR) 1-4

DSL Terminator profiles 1-4
- Obtaining privileges to use the menus 1-6
- Activating a profile 1-6

Configuring the DSL Terminator to use RADIUS 1-7
Where to go next 1-9

Chapter 2 Setting Up Security 2-1

What this chapter does not contain 2-1
What you should know 2-1
Getting started: Basic security measures 2-2
- Introducing Security profiles 2-2
- Understanding basic security measures 2-3
- Activating the Full Access profile 2-3
- Changing the Full Access profile password 2-4
- Setting the Default profile for read-only access 2-5
- Changing the SNMP read-write community string 2-6

Assigning a Telnet password 2-6
Requiring profiles for incoming connections 2-6
Turning off ICMP redirects 2-7
Specifying the number of retry attempts 2-7
Retrieving configuration updates from RADIUS 2-7
Setting up Security profiles 2-8
Configuring a Security profile 2-10
Activating a Security profile 2-13
Using the Full Access profile 2-13
Configuring the DSL Terminator to recognize the authentication server 2-14
Setting up user authorization 2-14
Setting up terminal-server security 2-15
Turning terminal-server operation on or off 2-15
Dealing with unauthorized Telnet and terminal-server sessions 2-16
Enabling the RADIUS Boot server 2-16
Setting up SNMP security 2-17
Password-protecting SNMP 2-18
Configuring the SNMP manager to use SNMP authentication 2-19
Setting up SNMP traps 2-19
Restricting the hosts that can issue SNMP commands 2-21
Setting up a Domain Name System (DNS) 2-22
Setting global DNS parameters 2-23
Setting client DNS parameters 2-24
Example of DNS configuration 2-24
Disabling remote management access 2-25
Password-protecting Telnet access 2-25
Limiting access to services and protocols 2-25

Chapter 3 Configuring WAN Access 3-1

Introduction to WAN configuration 3-1
Menus and profiles 3-1
How the VT100 menus relate to slots and ports 3-1
System slot 3-1
WAN slots 3-2
Ethernet and WAN slots 3-3
Configuring DS3-ATM connections 3-3
Configuring DS3-ATM lines 3-4
Configuring IP over ATM 3-5
Configuring the ATM card 3-5
Configuring the Connection profile for the remote device 3-6
Configuring UDS3 connections and lines 3-6
Configuring the OC3-ATM connections 3-7
Net/OC3-SMF-ATM (Net/OC3-UTP-ATM) profile 3-8
Configuring the OC3-ATM lines 3-9
Example of an IP over OC3-ATM configuration 3-10
Configuring an IP-over-ATM PVC connection 3-10
Traffic shaping for ATM cards 3-12
Configuring T1 lines 3-15
Configuring the nailed T1 line 3-16
Using T1 line diagnostics 3-17
Configuring E1 lines 3-18
E1 framing 3-18

Clock source for synchronous transmission 3-18
How the DS0s are used 3-18
Configuring the nailed E1 line 3-18
Using E1 line diagnostics 3-20

Chapter 4 Configuring Individual WAN Connections 4-1

Understanding the Answer profile 4-1
Understanding Connection profiles 4-4
Connection profile parameters 4-6
Encapsulation options 4-6
Encaps Options subprofile parameters 4-8
Connection profile: Ip Options subprofile parameters 4-11
Connection profile: Session options subprofile 4-12
Connection profile: Telco Options subprofile 4-13
Connection profile: Accounting subprofile parameters 4-15
Understanding Names/Passwords profiles 4-15
Names and Passwords profile parameters 4-16
Example Names/Passwords profile configuration 4-16
Configuring PPP connections 4-16
Understanding the PPP Options subprofile parameters 4-18
Example of a PPP connection 4-20
Setting up a PPP connection using RADIUS 4-21
Before you begin 4-21
Configuring a PPP connection in RADIUS 4-22
PPP connection example 4-23
Setting up an MP or MP+ connection using RADIUS 4-24
Before you begin 4-24
Setting up a BACP connection 4-26
Configuring PPP over Ethernet (PPPoE) 4-26
Configuring PPPoE on an Ethernet interface 4-28
Configuring PPPoE over the WAN 4-28
Understanding PPPoE parameters 4-29
Settings in a RADIUS profile 4-29
RADIUS example 4-30
Configuring PPP over ATM 4-30
Configuring a PPP over ATM connection 4-31

Chapter 5 Configuring Frame Relay 5-1

Introduction 5-1
Frame Relay link management 5-2
Using the DSL Terminator as a Frame Relay concentrator 5-2
Using the DSL Terminator as a Frame Relay switch 5-3
Components of a Frame Relay configuration 5-3
Configuring nailed bandwidth for Frame Relay 5-3
Managing bandwidth using RADIUS 5-4
Setting up a nailed-up connection using RADIUS 5-5
Configuring a nailed-up connection in RADIUS 5-6
Nailed-up connection example 5-7
Modifying or deleting nailed-up profiles 5-7
Defining Frame Relay link operations 5-7
Understanding Frame Relay parameters 5-7

Settings in a RADIUS frdlink profile 5-10
Configuring a DLCI logical interface 5-15
Overview of DLCI interface settings 5-15
Settings in a Connection profile 5-15
Understanding the Frame Relay connection parameters 5-17
Settings in a RADIUS profile 5-17
Examples of a DLCI interface configuration 5-18
Examples of backup interfaces for nailed Frame Relay links 5-19
Configuring the DSL Terminator as a Frame Relay switch 5-21
Overview of circuit-switching parameters 5-21
Settings in a Connection profile 5-21
Settings in a RADIUS profile 5-22
Examples of a circuit between UNI interfaces 5-22
Examples of a circuit between NNI interfaces 5-24
Examples of circuits that use UNI and NNI interfaces 5-26
Frame Relay and ATM internetworking support 5-30
FRF.8 Configuration 5-30

Chapter 6 Configuring IP Routing 6-1

Introduction to IP routing and interfaces 6-1
IP addresses and subnet masks 6-1
Zero subnets 6-3
IP routes 6-4
How the DSL Terminator uses the routing table 6-4
Static routes 6-4
Dynamic routes 6-4
Route preferences and metrics 6-4
DSL Terminator IP interfaces 6-5
Ethernet interfaces 6-5
WAN IP interfaces 6-6
Numbered interfaces 6-6
Configuring the local IP network 6-7
Understanding IP network parameters 6-9
Ethernet interface IP addresses 6-9
Enabling RIP on the Ethernet interface 6-10
Ignoring the default route 6-10
Proxy ARP and inverse ARP 6-10
Configuring system-level routing policies 6-11
Dynamic IP addressing for dial-in hosts 6-11
Enabling dynamic address assignment 6-11
Specifying address pools 6-11
Forcing callers configured for a pool address to accept dynamic assignment 6-12
Summarizing host routes in routing table advertisements 6-12
Boot Protocol (BOOTP) requests to other networks 6-16
Name resolution service (DNS or WINS) 6-16
IP network configuration examples 6-19
Configuring the DSL Terminator IP interface on a subnet 6-19
Configuring DNS 6-20
Additional terminal-server commands 6-21
Show commands 6-21
DNStab commands 6-22
Configuring the local DNS table 6-22

Criteria for valid names in the local DNS table 6-22
Entering IP addresses in the local DNS table 6-22
Editing the local DNS table 6-23
Deleting an entry from the local DNS table 6-24
Configuring IP routing connections 6-24
Understanding IP routing connection parameters 6-25
Configuring the remote IP address 6-25
Assigning metrics and preferences 6-26
Checking remote host requirements 6-27
UNIX software 6-27
Window or OS/2 software 6-27
Macintosh software 6-27
Software configuration 6-27
Examples of IP routing connections 6-28
Configuring a host connection with a static address 6-28
Configuring a router-to-router connection 6-29
Configuring a router-to-router connection on a subnet 6-30
Configuring a numbered interface 6-32
Configuring IP routes and preferences 6-33
Understanding the static route parameters 6-33
Configuring the default route 6-38
Defining a static route to a remote subnet 6-38
Example of route preferences configuration 6-39
Configuring static IP routes in RADIUS 6-39
Configuring dynamic route updates 6-43
Dynamic route configuration 6-43
Example of RIP and ICMP configuration 6-44

Chapter 7 Configuring OSPF Routing 7-1

OSPF overview 7-1
TAOS implementation of OSPF 7-2
OSPF features 7-2
Security 7-2
Support for variable length subnet masks 7-3
Exchange of routing information 7-3
Designated and Backup Designated Routers 7-4
Configurable metrics 7-4
Hierarchical routing (areas) 7-5
Stub areas 7-6
Not So Stubby Areas (NSSAs) 7-6
The link-state routing algorithm 7-7
Configuring OSPF routing in the DSL Terminator 7-8
Understanding the OSPF routing parameters 7-9
Examples of configurations for adding the DSL Terminator to an OSPF network 7-12
Configuring OSPF on the Ethernet interface 7-12
Configuring OSPF across the WAN 7-14
Configuring a WAN link that does not support OSPF 7-15

Chapter 8 Configuring Packet Bridging 8-1

Introduction to bridging 8-1
Disadvantages of bridging 8-1

Initiating a bridged WAN connection 8-2
Physical addresses and the bridge table 8-2
Broadcast addresses 8-2
Establishing a bridged connection 8-2
Enabling bridging 8-3
Managing the bridge table 8-3
Transparent bridging 8-4
Bridge Groups 8-4
Sample DSL Terminator bridge group configuration 8-4
Configuring a bridge group on an Ethernet interface 8-6
Configuring the Connection profile for a bridge group 8-6
Configuring additional Connection profiles from existing profiles 8-7
RADIUS user profile for bridge groups 8-7
Example of a DSL Terminator bridge group configuration 8-7
Configuring a bridge group on an Ethernet interface 8-9
Configuring the SDSL profile 8-9
Configuring the Connection profile 8-9
Configuring additional Connection profiles from existing profiles 8-10
Bridged IP routing 8-11
Overview of bridged IP routing 8-11
Example of a DSL Terminator bridged IP routing with subnets configuration 8-12
Configuring the Frame Relay profile 8-13
RADIUS user profile for bridged IP routing with subnets 8-14
Example of a DSL Terminator bridged IP routing with host routes configuration 8-14
Configuring a Connection profile 8-16
RADIUS user profile for bridged IP routing with host routes 8-17
Designating egress interfaces for bridged IP routing or bridge groups 8-17
Parameter and RADIUS attribute reference 8-18
Restricting multicast bridging 8-18
Overview of RADIUS bridging attributes 8-19
Specifying protocol-independent bridging 8-19
Configuring bridge entries 8-19
Bridge profile configuration examples 8-21

Chapter 9 Setting Up IP Multicast Forwarding 9-1

Introduction to multicast forwarding 9-1
Configuring multicast forwarding 9-2
Enabling multicast forwarding 9-2
Identifying the MBONE interface 9-2
Multicast forwarder polling activities 9-2
Configuring the DSL Terminator to support multicast clients 9-2
Specifying the interfaces that support multicast clients 9-2
Specifying the rate which multicast clients accept packets 9-3
Querying for active group members 9-3
Multicast interfaces 9-3
Implicit priority setting for dropping multicast packets 9-4
Monitoring connectivity problems through heartbeat monitoring 9-4
Examples of multicast forwarding configuration 9-5
Forwarding from an MBONE router on Ethernet 9-5
Forwarding from an MBONE router on a WAN link 9-6
Configuring the DSL Terminator to respond to multicast clients 9-7
Configuring the MBONE interface 9-7

Configuring multicasting on WAN interfaces 9-7
Restricting multicast bridging 9-8
Setting up multicast forwarding using RADIUS 9-8
Configuring multicast forwarding in RADIUS 9-8

Chapter 10 Configuring Virtual Private Networks 10-1

Introduction to virtual private networks 10-1
Creating and Configuring ATMP tunnels 10-1
How the DSL Terminator creates ATMP tunnels 10-2
Setting the UDP port 10-3
Setting an MTU limit 10-3
Forcing fragmentation for interoperation with outdated clients 10-4
Router and gateway mode 10-5
Overview of RADIUS attributes for ATMP 10-5
Configuring a Foreign Agent 10-6
Understanding the Foreign Agent parameters and attributes 10-8
Example of configuring a Foreign Agent (IP) 10-9
Setting an idle timer for unused tunnels 10-19
Configuring the DSL Terminator as an ATMP multimode agent 10-19
Supporting Mobile Client routers (IP only) 10-22
ATMP connections that bypass a Foreign Agent 10-23
Configuring PPTP tunnels 10-23
How the DSL Terminator works as a PAC 10-23
Understanding the PPTP PAC parameters 10-24
Enabling PPTP 10-24
Specifying a PRI line for PPTP calls and the PNS IP address 10-24
Example of a PAC configuration 10-24
Example of a PPTP tunnel across multiple POPs 10-25
Routing a terminal-server session to a PPTP server 10-26
Configuring L2TP tunnels 10-27
Elements of L2TP tunneling 10-27
How the DSL Terminator creates L2TP tunnels 10-28
LAC and LNS mode 10-28
Tunnel authentication 10-29
Client authentication 10-29
Flow control 10-29
Understanding the L2TP LAC parameters 10-30
Configuring the DSL Terminator as an LNS 10-32
Configuring L2TP Mobile Client profiles 10-32
L2TP settings in RADIUS profiles 10-32
Configuring Virtual Routers 10-33
Current limitations 10-33
Creating a Virtual Router profile 10-34
Required Virtual Routers profile settings 10-34
Required Connection profile settings 10-34
Required Static Rtes profile settings 10-35
Disabling a Virtual Router profile 10-35
Understanding VRouter parameters 10-35

Chapter 11 Defining Static Filters 11-1

Introduction to filters 11-1

Basic types of filters 11-1
Data and call filters 11-2
How filters work 11-2
Generic filters 11-3
IP filters 11-3
Type of Service filters 11-4
Specifying a filter's direction 11-4
Specifying a filter's forwarding action 11-5
Defining generic filters 11-6
Settings in a local Filter profile 11-6
Settings in a RADIUS profile 11-7
Specifying the offset to the bytes to be examined 11-8
Specifying the number of bytes to test 11-8
Masking the value before comparison 11-9
Examples of a generic call filter 11-10
Defining IP filters 11-10
Settings in a local Filter profile 11-10
Settings in a RADIUS profile 11-12
Filtering by source or destination address 11-13
Filtering by port numbers 11-14
Examples of an IP filter to prevent local address spoofing 11-14
Examples of an IP filter for more complex security issues 11-15
Defining Type of Service filters 11-17
Settings in a local Filter profile 11-17
Settings in a RADIUS profile 11-19
Examples of defining a TOS filter 11-21
Applying a filter to an interface 11-22
Settings in local profiles 11-22
Settings in RADIUS profiles 11-23
How the system uses the Answer Default parameter 11-23
Examples of applying a data filter to a WAN interface 11-24
Examples of applying a call filter to a WAN interface 11-25
Examples of applying a TOS filter to a WAN interface 11-25
Example of applying a filter to a LAN interface 11-26

Index Index-1

Figures

Figure 3-1 Example of an DS3-ATM setup 3-3
Figure 3-2 IP over ATM 3-5
Figure 3-3 Example UDS3 setup 3-6
Figure 3-4 IP over ATM PVC connection 3-11
Figure 4-1 A PPP connection 4-21
Figure 4-2 An MP+ connection 4-24
Figure 4-3 Example of PPPoE configuration 4-27
Figure 4-4 Example PPP over ATM configuration 4-31
Figure 4-5 Example PPP over ATM configuration 4-32
Figure 5-1 Frame Relay network 5-2
Figure 5-2 Frame Relay concentrator 5-2
Figure 5-3 Frame Relay switch 5-3
Figure 5-4 Frame Relay DTE interface 5-12
Figure 5-5 Frame Relay DCE interface 5-13
Figure 5-6 Frame Relay NNI interface 5-14
Figure 5-7 Frame Relay PVC 5-18
Figure 5-8 Frame Relay circuit with UNI interfaces 5-23
Figure 5-9 Frame Relay circuit with NNI interfaces 5-24
Figure 5-10 Frame Relay circuit with UNI and NNI interface 5-26
Figure 6-1 Default mask for class C IP address 6-2
Figure 6-2 A 29-bit subnet mask and the number of supported hosts 6-2
Figure 6-3 Interface-based routing example 6-6
Figure 6-4 Sample dual IP network 6-10
Figure 6-5 Address assigned dynamically from a pool 6-14
Figure 6-6 Creating a subnet for the DSL Terminator 6-19
Figure 6-7 Local DNS table example 6-21
Figure 6-8 A user requiring a static IP address (a host route) 6-28
Figure 6-9 A router-to-router IP connection 6-29
Figure 6-10 A connection between local and remote subnets 6-30
Figure 6-11 Example of a numbered interface 6-32
Figure 6-12 Two-hop connection that requires a static route when RIP is off 6-39
Figure 6-13 A two-hop connection that requires a static route when RIP is off 6-42
Figure 7-1 Adjacency between neighboring routers 7-3
Figure 7-2 Designated and Backup Designated Routers 7-4
Figure 7-3 OSPF costs for different types of links 7-5
Figure 7-4 Dividing an AS into areas 7-6
Figure 7-5 Sample network topology 7-7
Figure 7-6 Example of an OSPF setup 7-12
Figure 8-1 Negotiating a bridge connection (PPP encapsulation) 8-3
Figure 8-2 How the DSL Terminator creates a bridging table 8-4
Figure 8-3 Example of a DSL Terminator bridge group configuration 8-5
Figure 8-4 Example of a bridge group configuration 8-8
Figure 8-5 DSL bridged environment 8-11

Figure 8-6 Sample bridged IP routing with subnets configuration 8-12
Figure 8-7 Bridged IP routing with host routes (BIR/32) 8-15
Figure 9-1 DSL Terminator forwarding multicast traffic to dial-in multicast clients 9-5
Figure 9-2 DSL Terminator forwarding multicast traffic to dial-in multicast clients 9-6
Figure 10-1 ATMP tunnel across the Internet 10-2
Figure 10-2 Path MTU on an Ethernet segment 10-3
Figure 10-3 Home Agent routing to the Home network 10-11
Figure 10-4 Home Agent in gateway mode 10-14
Figure 10-5 DSL Terminator acting as both Home Agent and Foreign Agent 10-19
Figure 10-6 PPTP tunnel 10-25
Figure 10-7 PPTP tunnel across multiple POPs 10-25
Figure 10-8 L2TP tunnel across the Internet 10-28
Figure 10-9 Typical VRouter implementation 10-33
Figure 11-1 Data filters drop or forward certain packets 11-2
Figure 11-2 Call filters prevent certain packets from resetting the timer 11-2

Tables

Table 1-1 Where to go next 1-9
Table 2-1 Security profile parameters 2-8
Table 2-2 Authentication server parameters 2-14
Table 2-3 Characters used in the terminal-server prompt specification 2-15
Table 2-4 SNMP security parameters 2-18
Table 2-5 DNS parameters 2-23
Table 2-6 Limiting services and protocols 2-25
Table 3-1 OC3-ATM line configuration tasks 3-8
Table 4-1 PPP attributes 4-22
Table 4-2 MP and MP+ attributes 4-25
Table 4-3 BACP attribute 4-26
Table 5-1 Bandwidth management attributes 5-4
Table 5-2 Nailed-up attributes 5-6
Table 6-1 IP address classes and number of network bits 6-2
Table 6-2 Standard subnet masks 6-3
Table 6-3 Framed-Route arguments 6-41
Table 7-1 Link-state databases for network topology in Figure 7-5 7-7
Table 7-2 Shortest-path tree and resulting routing table for Router-1 7-8
Table 7-3 Shortest-path tree and resulting routing table for Router-2 7-8
Table 7-4 Shortest-path tree and resulting routing table for Router-3 7-8
Table 8-1 Bridging attributes 8-19
Table 8-2 Ascend-Bridge-Address arguments 8-20
Table 9-1 Multicast forwarding attributes 9-8
Table 10-1 RADIUS attributes required for ATMP connections 10-5
Table 10-2 Required RADIUS attributes to reach an IP Home network 10-8
Table 10-3 RADIUS attributes for specifying L2TP tunnels 10-31

About This Guide

What is in this guide

This guide explains how to configure and use the DSL Terminator product. Following is a chapter-by-chapter description of the topics:

- Chapter 1, “Getting Acquainted with the DSL Terminator,” describes the DSL Terminator.
- Chapter 2, “Setting Up Security,” explains configuring and administering security for your network.
- Chapter 3, “Configuring WAN Access,” shows you how to configure the DSL Terminator for various types of WAN connectivity.
- Chapter 4, “Configuring Individual WAN Connections,” explains how to set up your connections for PPP, MP+, or Frame Relay protocols.
- Chapter 5, “Configuring Frame Relay,” explains how to set up your connections for Frame Relay.
- Chapter 6, “Configuring IP Routing,” explains how to configure the DSL Terminator for IP routing.
- Chapter 7, “Configuring OSPF Routing,” explains how to configure the DSL Terminator for OSPF routing.
- Chapter 8, “Configuring Packet Bridging,” explains how to configure the DSL Terminator for bridging.
- Chapter 9, “Setting Up IP Multicast Forwarding,” explains how to configure the multicast forwarding.
- Chapter 10, “Configuring Virtual Private Networks,” explains how to configure the DSL Terminator for a Virtual Private Network.
- Chapter 11, “Defining Static Filters,” explains how filters work and how to define filters.

This guide also includes an index.

Caution: 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 guide is for the person who configures and maintains the DSL Terminator. To configure the DSL Terminator, you need to understand the following:

- Wide area network (WAN) concepts
- Local area network (LAN) concepts, if applicable

Documentation conventions

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

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

Note: In a menu-item path, include a space before and after each ">" character.

Manual Set

The *DSL Terminator* Documentation Set consists of the following manuals:

- *DSL Terminator Administration Guide*
- *DSL Terminator Hardware Installation Guide*

- *DSL Terminator Network Configuration Guide* (this book)
- *DSL Terminator Reference*
- *TAOS RADIUS Guide and Reference*
- *TAOS Glossary*
- *Access Networks Safety and Compliance Guide*

Related publications

This guide and documentation set do not provide a detailed explanation of products, architectures, or standards developed by other companies or organizations.

Here are some related publications that you may find useful:

- *The Guide to T1 Networking, William A. Flanagan*
- *Data Link Protocols, Uyless Black*
- *The Basics Book of ISDN, Motorola University Press*
- *ISDN, Gary C. Kessler*
- *TCP/IP Illustrated, W. Richard Stevens*
- *Firewalls and Internet Security, William R. Cheswick and Steven M. Bellovin*

Getting Acquainted with the DSL Terminator

1

Overview of DSL Terminator configuration 1-1

Management features 1-3

DSL Terminator profiles 1-4

Configuring the DSL Terminator to use RADIUS. 1-7

Where to go next 1-9

Overview of DSL Terminator configuration

Before you configure the DSL Terminator, you should create a network diagram. Configuration tasks generally consist of:

- Configuring the lines, channels, and ports, and how calls are routed between them
- Configuring wide area network connections and security
- Configuring the DSL Terminator as a Frame Relay concentrator
- Configuring routing and bridging across the WAN

Creating a network diagram

Lucent Technologies strongly recommends that, after you have read these introductory sections, you diagram your network and refer to the diagram while configuring the DSL Terminator. Creating a comprehensive network diagram helps prevent problems during installation and configuration, and can help in troubleshooting any problems later.

Configuring lines, slots, and ports for WAN access

Once you enable the lines, slots, and ports for WAN access, you need to configure the way in which outbound calls are routed to them and the way in which inbound calls are routed from them to other destinations (such as the local network).

Configuring WAN connections and security

When the nailed connection establishes, software at both ends of the connection encapsulates each packet before sending it out over the phone lines. Each type of encapsulation supports its own set of options, which can be configured on a per-connection basis to enable the DSL Terminator to interact with a wide range of software and devices.

After a connection's link encapsulation method has been negotiated, the DSL Terminator typically uses a password to authenticate the call. For detailed information about authentication and authorization, see Chapter 2, "Setting Up Security." Following are some of the connection security features that the DSL Terminator supports:

Feature	Description
Authentication protocols	For PPP connections, the DSL Terminator supports both Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP). CHAP is more secure than PAP, and is preferred if both sides of the connection support it.
Authentication servers	You can offload the authentication responsibility to a RADIUS or TACACS server on the local network.
Filters and firewalls	Packet-level security mechanisms can provide a very high level of network security.

Concentrating Frame Relay connections

The DSL Terminator provides extensive support for Frame Relay. Using a T1 or E1 line or serial WAN port for a nailed connection to a switch, it can function as a network-to-network interface (NNI) switch, a data communications equipment (DCE) unit responding to users, or as a data terminal equipment (DTE) unit requesting services from a switch.

Configuring routing and bridging across the WAN

Routing and bridging configurations enable the DSL Terminator to forward packets between the local network and the WAN and also between WAN connections.

Enabling protocol-independent packet bridging

The DSL Terminator can operate as a link-level bridge, forwarding packets from Ethernet to a WAN connection (and vice versa) on the basis of the destination hardware address in each packet. Unlike a router, a bridge does not examine packets at the network layer. It simply forwards packets to another network segment if the address does not reside on the local segment.

IP routing

IP routing is the most widespread use of the DSL Terminator, and it has a wide variety of configurable options. IP routing is the required protocol for Internet-related services such as IP multicast support, and cross-Internet tunneling for virtual private networks. Most sites create static IP routes to enable the DSL Terminator to reliably bring up a connection to certain destinations or to change global metrics or preferences settings.

Configuring Internet services

All Internet services and routing methods require that the DSL Terminator function as an IP router, so an IP routing configuration is a necessary precondition.

Management features

The terminal-server command line provides access to management features that are not available through the menus. The VT100 window does, however, provide status information. The DSL Terminator supports SNMP, remote management, serial port software upgrades, and Call Detail Reporting (CDR).

The DSL Terminator provides up to nine security levels to control the management and configuration functions that are accessible to users. For more information on management features, see the *DSL Terminator Administration Guide*.

Using the terminal-server command line

To invoke the terminal server command-line interface, you must have administrative privileges. Once you have activated a Security profile that enables these privileges, you can invoke the command line by selecting Term Serv in the Sys Diag menu. To close the command line, use the Quit command at the command-line prompt. The command-line interface closes and the cursor returns to the VT100 menus. For detailed information on the terminal-server, see Chapter 4, “Configuring Individual WAN Connections.”

Using status windows to track WAN or Ethernet activity

The VT100 interface displays eight status windows to the right of the configuration menus. The windows provide a great deal of read-only information about what is currently happening in the DSL Terminator. If you want to focus on the activity of a particular slot card, you can change the default contents of the windows to show what is currently occurring in that slot.

Using SNMP to manage the unit

Many sites use Simple Network Management Protocol (SNMP) applications to obtain information about the DSL Terminator and make use of it to enhance security, set alarms for certain conditions, and perform simple configuration tasks.

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

Using remote management to configure far-end units

When you have an MP+ or AIM connection to another DSL Terminator, you can use the management subchannel established by those protocols to control, configure, and obtain statistical and diagnostic information about that unit. Multilevel password security ensures that unauthorized personnel do not have access to remote management functions.

Flash RAM and software updates

Flash RAM technology enables you to perform software upgrades in the field without opening the unit or changing memory chips. You can upgrade the DSL Terminator through its serial port by accessing it locally. You cannot perform remote software upgrades over the WAN interface because of a conflict between running the WAN and reprogramming the software.

Call Detail Reporting (CDR)

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

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

DSL Terminator profiles

A profile is a group of related settings that appears on the VT100 interface. To navigate the interface, use the arrow keys or Control-key combinations as described in the *DSL Terminator Hardware Installation Guide*. When you first telnet to the VT100 interface, the Main Edit Menu typically appears:

```
Main Edit Menu
 00-000 System
>10-000 Net/8T1
 20-000 Net/8T1
 30-000 Ethernet
```

The items in the Main Edit Menu open submenus, many of which have submenus. The 10-100 Net/8T1 and 20-000 Net/8T1 items, for example, represent the two T1 slots on the unit. (If your unit has E1 slots instead, the item names are 10-100 Net/8E1 and 20-000 Net/8E1.) By selecting one of these two items, you open a submenu from which you can select line configuration or line diagnostics:

```
10-000 Net/8T1
  10-100 Line Config
  20-100 Line Diag
```

If you select line configuration, a list of slot-configuration profiles appears:

```
10-100 Line Config
 10-1** Factory
   10-101
```

```
   10-102
   10-103
   10-104
```

Each of the slot-configuration profiles provides access to the same set of parameters. You can configure multiple profiles to create alternative configurations for the slot:

```
10-101
>Name=
 Line 1...
 Line 2...
 Line 3...
 Line 4...
 Line 5...
 Line 6...
 Line 7...
 Line 8...
```

The eight submenus (Line 1 through Line 8, often referred to collectively as Line *N*) provide access to the parameters for configuring the eight lines, respectively, of the slot. For example, if you select Line 1, the following set of parameters appears:

```
10-101
 Line 1...
>Enabled=
 Nailed Group=
 Framing Mode=
 Front End=
 Encoding=
 Length=
 Buildout=
 Clock Source=
 First DS0 channel=
 Last DS0 channel=
```

In this manual, an instruction to access a parameter in the Line 1 profile is written as follows:

Net/8T1 > Line Config > (*any*) *slot profile* > *parameter name*

In an example of the settings in a profile, levels of indentation represent the levels of nested subprofiles. For example, a Net/8T1 > Line Config > *any slot profile* > Line *N* profile could be shown as follows:

```
Net/8T1
 Line Config
  any slot profile
   Line N
   Enabled=
   Nailed Group=
   Framing Mode=
   Front End=
   Encoding=
   Length=
```

```
Buildout=
Clock Source=
First DS0 channel=
Last DS0 channel=
```

Obtaining privileges to use the menus

As explained in the *DSL Terminator Hardware Installation Guide*, privileges are often required for changing settings in the unit's menus. To activate a profile, for example, you need full privileges. Unless you have a personal profile that grants full privileges, activate the Full Access profile, as follows:

1 At the Main Edit Menu, press Ctrl-D.
The Main Edit Menu's DO menu appears.

2 Select P (Password).

3 Press Enter or the Right-Arrow key.
The Security Profile menu appears.

4 Select Full Access.

5 Press Enter or the Right-Arrow key.
A password entry field appears.

6 Enter your password within the brackets.

7 Press Enter or the Right-Arrow key.
If your password is accepted, you have Full Access privileges.

8 Press Enter.
The Main Edit Menu reappears.

Activating a profile

After you have full privileges as described in the previous procedure, you can now make a profile (such as one of the slot-configuration profiles described on page 1-4) active. Proceed as follows:

1 Open the profile that you want to make current.

2 Press Ctrl-D.
The profile's DO menu appears.

3 Select L (Load).
The Load Profile menu appears.

4 Select 1 to load the profile.
`Profile loaded as current profile` appears.
The profile reappears.

Configuring the DSL Terminator to use RADIUS

This section describes how to configure the DSL Terminator unit to communicate with the RADIUS daemon.

Note: This section describes the basic configuration procedure. It does not cover how to configure RADIUS for accounting purposes. For information on setting up accounting, see the *TAOS RADIUS Guide and Reference*.

1. Open the Ethernet menu.
2. Open the Mod Config menu.
3. Open the Auth menu.
4. Set the Auth parameter to RADIUS or RADIUS/LOGOUT.

   If you set Auth=RADIUS/LOGOUT, RADIUS keeps track of session logouts.
5. For each Auth Host parameter, specify the IP address of a RADIUS server.

   You can have up to three RADIUS servers on your network. One is the primary server. Two additional servers can serve as backups. If the primary RADIUS server fails, the DSL Terminator unit automatically contacts the secondary RADIUS server to authenticate a user.

   The DSL Terminator unit first tries to connect to Auth Host #1. If it receives no response within the time specified by the Auth Timeout parameter, it tries to connect to Auth Host #2. If it again receives no response within the time specified by Auth Timeout, it tries to connect to Auth Host #3. If the DSL Terminator unit's request again times out, it reinitiates the process with Auth Host #1. The DSL Terminator unit can complete this cycle of requests a maximum of ten times.

   When it successfully connects to an authentication server, the DSL Terminator unit uses that machine until it fails to serve requests. By default, the DSL Terminator unit does not use the first host until the second machine fails, even if the first host has come online while the second host is still servicing requests. However, you can use SNMP to specify that the DSL Terminator unit use the first host again. For details, see "Using SNMP to specify the primary RADIUS server" on page 2-22.

   You can also specify the same address for all three Auth Host parameters. If you do so, the DSL Terminator unit keeps trying to create a connection to the same server.
6. For the Auth Port parameter, enter the UDP port number you specified for the daemon in the `/etc/services` directory.

   The DSL Terminator and the daemon must agree about which UDP port to use for communication, so make sure that the number you specify for the Auth Port parameter matches the number specified for the daemon.
7. To specify the number of seconds the DSL Terminator unit waits for a response to a RADIUS authentication request, set the Auth Timeout parameter.

   If the DSL Terminator unit does not receive a response within the time specified by Auth Timeout, it sends the authentication request to the next authentication server specified by the Auth Host parameter.

   By default, if authentication fails on a PPP connection because of a bad password or an authentication server timeout, the DSL Terminator unit gracefully shuts down the PPP connection by sending an LCP-CLOSE request to the dial-in host. When Windows 95 (MSN) receives the LCP-CLOSE during authentication, it assumes a rejected password, and displays a message telling the user that his or her password is invalid. If authentication fails because of a RADIUS timeout, this message gives the user incorrect information.

To specify that the DSL Terminator unit simply hangs up a PPP connection on a RADIUS timeout without closing down cleanly, set Disc on Auth Timeout=Yes in the Answer profile. The resulting message to the user specifies that the network failed.

8 For the Auth Key parameter, enter the RADIUS client password exactly as it appears in the RADIUS `clients` file.

The password is case sensitive.

9 Set the Auth Pool parameter to specify whether the DSL Terminator unit sends the IP address from pool #1 to the RADIUS server when it requests authentication.

For information on the Auth Pool parameter, see the *TAOS RADIUS Guide*.

10 To specify information about the host running the APP Server utility, set the APP Server, APP Host, and APP Port parameters.

For more information, see the *TAOS RADIUS Guide*.

11 To configure the DSL Terminator unit to recognize a security-card authentication server, set the Password Server and Password Port parameters.

For more information, see "Configuring the DSL Terminator to recognize the authentication server" on page 2-14.

12 To specify whether the DSL Terminator unit first checks for a local Connection profile when attempting to authenticate a connection, set the Local Profile First parameter.

You can specify either Yes or No.

- Yes indicates that the DSL Terminator checks for a local Connection profile, and then a remote profile when attempting to authenticate a connection.

  Yes is the default.

- No indicates that the DSL Terminator unit checks for a remote profile, then a local Connection profile when attempting to authenticate a connection.

13 Set the Sess Timer parameter (if Auth=RADIUS/LOGOUT).

The DSL Terminator can report the number of sessions by class to a RADIUS authentication server when Auth=RADIUS/LOGOUT. The Sess Timer parameter specifies the interval in seconds in which the DSL Terminator unit sends session reports. You can specify a number between 0 and 65535.The default value is 0 (zero), which indicates that the DSL Terminator unit does not send reports on session events.

14 To specify the source port to use for sending a remote authentication request, set the Auth Src Port parameter.

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. You can specify the same source port for authentication and accounting requests.

15 Set the Auth Send Attr 6, 7 parameter.

This parameter specifies whether the DSL Terminator unit sends values for the User-Service (6) and Framed-Protocol (7) attributes in Access-Request packets to the RADIUS server. While some RADIUS servers require these attributes in authentication requests, other RADIUS servers should not receive them.

Set this value to Yes if you want to generate the appropriate values for attributes 6 and 7 for an incoming call and send them in authentication requests to the RADIUS server. For example, if you set Auth Send Attr 6, 7=Yes, the DSL Terminator unit sets User-Service=Framed-User and Framed-Protocol=PPP for incoming PPP calls. The default value is Yes.

Set this value to No if your RADIUS server does not require attributes 6 and 7 in authentication requests.

16 Save your changes.

Where to go next

When you have planned your network, you are ready to configure the DSL Terminator. Its flexibility and its ever-increasing number of configurations means that there is no set order for configuration. You can perform configuration tasks in the order you prefer. Table 1-1 shows where to look for the information you need.

Table 1-1. Where to go next

To do this:	Go to this chapter or document:
Configuring security	Chapter 2, “Setting Up Security”
Configure slots, lines, and ports	Chapter 3, “Configuring WAN Access”
Configure WAN connections	Chapter 4, “Configuring Individual WAN Connections”
Set up Frame Relay	Chapter 5, “Configuring Frame Relay”
Set up IP routing	Chapter 6, “Configuring IP Routing”
Set up OSPF routing	Chapter 7, “Configuring OSPF Routing”
Set up packet bridging	Chapter 8, “Configuring Packet Bridging”
Set up Multicast Forwarding	Chapter 9, “Setting Up IP Multicast Forwarding”
Set up VPN	Chapter 10, “Configuring Virtual Private Networks”
Set up data and call filters	Chapter 11, “Defining Static Filters”
Work with status windows	*DSL Terminator Reference*
Write configuration scripts	*DSL Terminator Administration Guide*
Set up RADIUS	*TAOS RADIUS Guide and Reference*

Setting Up Security

2

This chapter guides you in configuring security on the DSL Terminator. It explains how to set up different kinds of security by options using the DSL Terminator configuration interface.

What this chapter does not contain 2-1

What you should know 2-1

Getting started: Basic security measures 2-2

Setting up Security profiles 2-8

Setting up user authorization 2-14

Limiting access to services and protocols 2-25

What this chapter does not contain

This chapter does not describe how to set up security in RADIUS or how to use the NavisRadius™ product. Further, it does not discuss general network security issues or provide guidelines about the extent to which you should protect your network and local hosts. For pointers to information about these products and topics, consult the following publications:

Topic	Publication
RADIUS	*TAOS RADIUS Guide and Reference*
NavisRadius™	*NavisRadius Guide and Reference*
Detailed discussion of security issues	*Firewalls and Internet Security* by William R. Cheswick and Steven M. Bellovin

What you should know

You should read this chapter if you are configuring security in the DSL Terminator. This chapter does not discuss general network security issues, or provide guidelines for protecting your network and local hosts. To use this chapter effectively, however, you should be familiar with network security. If you need background information, you might find the book by William R. Cheswick and Steven M. Bellovin helpful. (For a list of publications, see “What this chapter does not contain” on page 2-1.)

You might also want to consider RADIUS and other external servers that offer additional methods for handling security.

Lucent's Access Control is a software program that provides authentication, authorization, and accounting services for users who request network connections.

Getting started: Basic security measures

This section describes how to set up basic security on the DSL Terminator.

Introducing Security profiles

To control access to the DSL Terminator, you configure parameters in Security profiles. All Security profiles are located below the Security menu of the System profile in the DSL Terminator configuration interface.

```
00-300 Security
  00-301 Default
  00-302
  00-303
  00-304
  00-305
  00-306
  00-307
  00-308
  00-309 Full Access
```

All units provide the following special profiles:

Profile	Description
Full Access	Provides full access to the DSL Terminator. This is the superuser profile that enables you to configure your system, reset the unit, and upgrade system software. Any user who knows the password for the Full Access profile can perform any operation on the DSL Terminator. The default Full Access password is `Ascend`. To maintain security, you should change the Full Access password from its default value. For details, see "Changing the Full Access profile password" on page 2-4.
Default	The DSL Terminator assigns the Default profile to every user who logs in via Telnet, the Control port, and remote management. The DSL Terminator activates the Default profile when it powers on or resets. The privileges set in the Default profile are available to all users. You cannot change the name of the Default profile or assign a password to it. However, you can change its settings to make the profile more restrictive. For details, see "Setting the Default profile for read-only access" on page 2-5.

Note: Follow the instructions in "Changing the Full Access profile password" on page 2-4 and "Setting the Default profile for read-only access" on page 2-5. These instructions result in two security levels, one that is totally open (Full Access) and one that is very restrictive (Default).

If you are the only user who must configure the DSL Terminator or perform administrative tasks, you do not need to create any Security profiles in addition to the Default and Full Access profiles. However, you can define additional security levels allowing specific users to perform a subset of administrative functions. You can create up to seven additional Security profiles. For more information about these tasks, see “Setting up Security profiles” on page 2-8.

Understanding basic security measures

When you first receive the DSL Terminator, all levels are set with full privileges. Initially, you can activate only the Default and Full Access profiles. Before you can activate one of the other Security Profiles, you must assign it a name. The default security settings of the Full Access profile enable you to configure and set up the DSL Terminator without any restrictions. Before you make the DSL Terminator generally accessible, you should protect the configured unit from unauthorized access. Proceed as follows:

1 Activate the Full Access profile.

2 Change the Full Access password.

3 Set the Default profile for read-only access.

4 Change the SNMP read-write community string.

5 Assign a Telnet password.

6 Require profiles for incoming connections.

7 Turn off ICMP redirects.

8 Specify the number of times the DSL Terminator retries a connection.

9 Retrieving configuration updates from RADIUS.

Activating the Full Access profile

You must activate the Full Access profile for your own use in performing the rest of the basic security measures. To activate the Full Access profile, proceed as follows:

1 From any VT100 menu, press <Ctrl> D.

The DO menu appears. For example:

```
DO...
>0=Esc
 P=Password
 C=Close TELNET
```

2 Press P or select P=Password.

A menu appears listing all security profiles:

```
Security profile...
  00-301 Default
  00-302 test
  00-303
  00-304
  00-305
  00-306
  00-307
  00-308
  00-309 Full Access
```

3 Select Full Access.

The DSL Terminator displays a password prompt.

4 Enter the password assigned to the Full Access security profile.

If you enter the correct password, the DSL Terminator displays the following message:

```
Password accepted. Using new security level.
```

If you enter the incorrect password, the unit prompts you again for the password.

Changing the Full Access profile password

The Full Access Security profile is the *superuser* profile that enables you to configure your system, reset the unit, and upgrade system software. Because this profile allows complete access, all privileges are set to Yes. The default password assigned to the profile is `Ascend`. A user who knows the password for the Full Access profile can perform any operation on the DSL Terminator.

Change the default password as soon as possible.

To assign a password protecting the Full Access profile, proceed as follows:

1 From any VT100 menu, press Ctrl-D.

The DO menu appears. For example:

```
DO...
  0=Esc
  P=Password
  C=Close TELNET
```

2 Press P or select P=Password.

A menu appears listing all security profiles:

```
Security profile...
  00-301 Default
  00-302 test
  00-303
  00-304
  00-305
  00-306
  00-307
  00-308
  00-309 Full Access
```

3 Select Full Access.

The unit displays a password prompt.

4 Enter the password assigned to the Full Access security profile.

If you enter the correct password, the unit displays the message `Password accepted. Using new security level.` If you enter the incorrect password, the unit prompts you again for the password.

5 Open the System > Security > Full Access profile.

6 Select the Passwd parameter and press Enter to open a text field.

7 Type a new password, and press Enter.

8 Exit the Full Access profile, and select the Exit and Accept option to save your changes.

Setting the Default profile for read-only access

The first profile in the Security menu is called `Default`. It has no password, and you cannot modify the profile's name or create a password. The DSL Terminator activates this profile whenever you power the unit on, reset the unit, or whenever a user begins a new login session.

Although the Default profile is set initially with full privileges, it is intended to be very restrictive. Every user who logs in via Telnet, the Control port, or remote management is granted the privileges specified there.

To make the Default profile appropriately restrictive, proceed as follows:

1 Open the System > Security menu.

2 Open the Default profile.

You cannot change the first two parameters in the Default profile. The name is always Default and the password is always null.

3 Set Operations parameter to No.

```
00-301 Default
 Name=Default
 Passwd=
>Operations=No
 Edit Security=N/A
 Edit System=N/A
 Edit Line=N/A
 Edit All Ports=N/A
 Edit Own Port=N/A
 Edit All Calls=N/A
 Edit Com Call=N/A
 Edit Own Call=N/A
 Edit Cur Call=N/A
 Sys Diag=N/A
 All Port Diag=N/A
 Own Port Diag=N/A
 Download=N/A
 Upload=N/A
 Field Service=N/A
```

All other parameters are set to N/A when the Operations parameter is set to No.

Users who access the DSL Terminator terminal server cannot make any changes to its configuration or perform restricted operations. For all users with the Default security level, passwords (including the null password) are hidden by the string *SECURE* in the DSL Terminator's user interface.

4 Exit the Full Access profile, and select the Exit and Accept option to save your changes.

Changing the SNMP read-write community string

An Simply Network Management Protocol (SNMP) community string is an identifier that an SNMP manager application must specify before it can access the MIB (Management Information Base). The DSL Terminator has two community strings:

String	Function
Read Comm	The read community string has the value *public* by default. It enables an SNMP manager to perform read commands (get and get next) in order to request specific information.
R/W Comm	The read-write community string has the value *write* by default. It enables an SNMP manager to perform both read and write commands (`get`, `get next`, and `set`). Using these commands, the application can access management information, set alarm thresholds, and change settings on the DSL Terminator.

You cannot turn off SNMP write, so you must change the default read-write string to secure the DSL Terminator against unauthorized SNMP access. To change the read-write community string, proceed as follows:

1. Open the Ethernet > Mod Config > SNMP Options menu.
2. For the R/W Comm parameter, specify a text string containing up to 16 characters, as in the following example:

   ```
   R/W Comm=unique-string
   ```

3. Close the SNMP Options menu, and select the Exit and Accept option to save your changes.

Assigning a Telnet password

Until you assign a Telnet password, any local user who knows the DSL Terminator's IP address can start a Telnet session with the unit. When you assign a password, all users requesting incoming Telnet sessions (whether locally or from across the WAN) must enter the password.

To assign a Telnet password, proceed as follows:

1. Open the Ethernet > Mod Config menu.
2. For the Telnet PW parameter, specify a password containing up to 20 characters.
   For example, you might enter this setting:

   ```
   Telnet PW=telnet-pwd
   ```

3. Close the Mod Config menu, and select the Exit and Accept option to save your changes.

Requiring profiles for incoming connections

You can use the unit's Answer profile to build connections that do not require a name and password. Although some sites allow such connections, most sites impose much tighter restrictions. You should consider limiting incoming connections to those that have a configured Connection profile, Password profile, or RADIUS User profile.

You can configure the DSL Terminator to reject all incoming connections for which it finds no matching profile.

To require configured profiles for all incoming connections, proceed as follows:

1. Open the Ethernet > Answer menu.
2. To specify that a matching profile is required for incoming calls, set the Profile Reqd parameter to Yes.
3. Exit the Answer profile, and select the Exit and Accept option to save your changes.

Turning off ICMP redirects

Internet Control Message Protocol (ICMP) enables a unit to 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. It is possible to counterfeit ICMP Redirects and change the way a device routes packets. If the DSL Terminator is routing IP, Lucent recommends that you turn off ICMP redirects.

To configure the DSL Terminator to ignore ICMP redirect packets, proceed as follows:

1. Open the Ethernet > Mod Config menu.
2. Set the ICMP Redirects parameter to Ignore.
3. Save your changes.

Specifying the number of retry attempts

When a DSL Terminator attempts to make a connection and the attempt fails, the DSL Terminator continues to attempt to complete the connection. The number of retry attempts allowed without using call blocking is very large and successive retries can cause excessive charges, congestion, and performance problems. With call blocking, you can specify a maximum number of unsuccessful attempts. After the specified number of attempts have been made and failed, the blocking timer starts. The DSL Terminator continues to block further retries for a the length of time you specify.

To configuring call blocking, proceed as follows:

1. Open the Ethernet > Connections > *any Connection profile* > Session options menu.
2. Set `Block calls after` to the number of retry attempts the DSL Terminator allows when placing a call.
3. Set `Blocked duration` to the length of time the DSL Terminator continues to block calls.

Call blocking applies only to outgoing calls that are not answered by the far end. It does not apply to incoming calls or outgoing calls that connect and are immediately disconnected

Retrieving configuration updates from RADIUS

When you power up the unit, it can retrieve a potentially large quantity of configuration information from the RADIUS server. Some of the data on the RADIUS server can change during operation. You can direct the unit to retrieve this information in one of two ways:

- Using the Upd Rem Cfg command from the Sys Diag menu, you can instruct the unit to retrieve a fresh configuration.
- You can initiate a RADIUS configuration update by using the SNMP Set command. Use SNMP to poll the status of the update.

The SNMP variable sysConfigRadiusCmd allows an SNMP manager to initiate a RADIUS configuration retrieval of routes, IP pools, connection information, and terminal server banners. You can poll the status of the retrieval by getting the value of another SNMP variable, sysConfigRadiusStatus.

Setting up Security profiles

A Security profile consists of parameters you can set to control access to the unit. All Security profiles are located below the Security menu of the System profile in the DSL Terminator configuration interface. Table 2-1 lists the parameters in a Security profile.

Table 2-1. Security profile parameters

Parameter	Specifies	Possible values
Name	Name for the profile.	Text string of up to 16 characters. The default value is null.
Passwd	Password.	Text string of up to 20 characters. The default value is null.
Operations	Enable/disable read-only security.	Yes (the default) No
Edit Security	Level of privileges for editing Security profiles.	Yes (the default) No
Edit System	Level of privileges for editing the System profile and the Read Comm and R/W Comm parameters in the Ethernet profile.	Yes (the default) No
Edit Line	Administrator can/cannot edit Line profiles.	Yes (the default) No
Edit All Ports	Administrator can/cannot edit all Port profiles.	Yes (the default) No
Edit Own Port	Administrator can/cannot edit his or her own Port profile.	Yes (the default) No **Note:** The No setting is ineffective unless you set the Edit All Ports parameter to No.

Table 2-1. Security profile parameters (continued)

Parameter	Specifies	Possible values
Edit All Calls	Administrator can/cannot edit all the parameters in all Call profiles and Connection profiles.	Yes (the default) No No specifies that an administrator can edit only the Base Ch Count parameters in the current Call profile.
Edit Com Call	Administrator can/cannot edit Call profiles that are not specific to any serial host port (such profiles are known as common Call profiles.)	Yes (the default) No **Note:** The No setting is ineffective unless you set the Edit All Ports parameter to No.
Edit Cur Call	Indicates whether an administrator can/cannot edit all the parameters in the current Call profile.	Yes (the default) No No specifies that an administrator can edit only the Base Ch Count parameters in the current Call profile. To disable editing of the Base Ch Count parameters, you must set the Edit Cur Call parameter to No *and* the Edit All Calls parameter to No.
Edit Own Call	Administrator can/cannot edit the Call profile that defines the connection between the DSL Terminator and the unit being remotely managed over an AIM channel.	Yes (the default) No **Note:** The No setting is ineffective unless you set the Edit All Ports parameter to No.
Sys Diag	Indicates whether an administrator can/cannot perform all system diagnostics.	Yes (the default) No
All Port Diag	Indicates whether an administrator can/cannot perform all serial host port diagnostics.	Yes (the default) No
Own Port Diag	Indicates whether an administrator can/cannot perform port diagnostics for his or her own serial host port.	Yes (the default) No To completely disable the administrator's ability to perform diagnostics for his or her own port, set the Own Port Diag parameter No and the All Port Diag parameter to No.

Table 2-1. Security profile parameters (continued)

Parameter	Specifies	Possible values
Download	Indicates whether an administrator can/cannot download the configuration of the DSL Terminator using the Save Cfg command.	Yes (the default) No **Note:** Whether you choose Yes or No, a user cannot download passwords to another device.
Upload	Indicates whether an administrator can/cannot upload the DSL Terminator configuration from another device using the Restore Cfg command.	Yes (the default) No **Note:** When you save a configuration to file, passwords are not included in the download, so restoring from file clears all passwords in the unit.
Field Service	Level of privileges for performing field service operations, such as uploading new system software.	Yes (the default) No

Configuring a Security profile

To configure a Security profile, proceed as follows:

1. Open the System > Security menu.
2. Open any Security profile.
3. Set the Name parameter to a descriptive designation for the profile.

   You can enter up to 16 characters. For example:

   ```
   Name=Calabasas
   ```
4. Specify a password of up to 20 character for the Passwd parameter value.
5. Set the Operations parameter to enable or disable read-only security.

   Yes (the default value) allows a user to view DSL Terminator profiles and to change the value of any parameter.

   No permits a user to view DSL Terminator profiles, but not to change the value of any parameter. If you specify No, a user cannot access most DO commands. Only DO Esc, DO Close Telnet, and DO password are available.
6. Set the Edit Security parameter to grant or restrict the privilege to edit Security profiles.

   With the Yes setting, a user can edit Security profiles and access all other operations permitted in his or her active Security profile. In addition, all passwords in Security profiles are visible as text. This privilege is the most powerful one you can assign because it allows users to change their own privileges. The default value is Yes.

   No restricts privileges. When Edit Security parameter is set to No, all passwords are hidden by the string "*SECURE*."

   Note: Do not set the Edit Security parameter to No on all nine Security profiles. If you do, you cannot edit any of them.

7 Set the Edit System parameter to grant or restrict privileges to edit the System profile and the Ethernet profile.

With the Yes setting, an administrator can edit the System profile and edit the Read Comm and R/W Comm parameters in the Ethernet profile. The default value is Yes.

No restricts edit privileges.

8 Set the Edit System parameter to indicate whether an administrator can edit Line profiles.

With the Yes setting, an administrator to edit Line profiles. The default value is Yes.

No prevents an administrator from editing Line profiles.

9 Set the Edit All Ports parameter to indicate whether an administrator can edit all Port profiles.

With the Yes setting, an administrator can edit all Port profiles though local or remote management. The default value is Yes.

No specifies that an administrator cannot edit Port profiles.

10 Set the Edit Own Port parameter to indicate whether an administrator can edit his or her own Port profile.

With the Yes setting, an administrator can use remote management to edit the Port profile for the port that has been called. The default value is Yes.

No specifies that an administrator cannot edit his or her own Port profile. To keep an administrator from editing his or her own Port profile, you must set the Edit Own Port parameter No and set the Edit All Ports parameter to No.

11 Set the Edit All Calls parameter to indicate whether an administrator can edit all the parameters in all Call profiles and Connection profiles.

With the Yes setting, an administrator can edit all the parameters in all Call profiles and Connection profiles through Telnet, through local management (the Control port), or through remote management. The default value is Yes.

No specifies that an administrator can edit only the Base Ch Count parameter in the current Call profile. To disable editing of the Base Ch Count parameter, set the Edit All Calls parameter to No and the Edit Cur Call parameter to No.

12 Set the Edit Com Call parameter to indicate whether an administrator can edit Call profiles that are not specific to any serial host port.

Call profiles not specific to any serial host port are known as common Call profiles. Numbers 201 through 216 denote port-specific Call profiles. Numbers 217 through 232 denote common Call profiles.

With the Yes setting, an administrator can edit common Call profiles by local or remote management. The default value is Yes.

No specifies that an administrator cannot edit common Call profiles. To keep an administrator from editing common Call profiles, set the Edit Com Call parameter to No and the Edit All Calls parameter to No.

13 Set the Edit Own Call parameter to indicate whether an administrator can edit the Call profile that defines the connection between the user's DSL Terminator and the unit being remotely managed over an AIM channel

With the Yes setting, an administrator can edit the Call profile. The default value is Yes.

No specifies that an administrator cannot edit the Call profile. To keep an administrator from editing the Call profile between a local and a remotely managed unit, set the Edit Own Call parameter to No and Edit All Calls parameter to No.

14 Set the Edit Cur Call parameter to indicate whether an administrator can edit all the parameters in the current Call profile.

With the Yes setting an administrator can edit all the parameters in the current Call profile by local or remote management. Yes is the default.

No specifies that an administrator can edit only the Base Ch Count parameter in the current Call profile. To disable editing of the Base Ch Count parameter, set Edit Cur Call parameter to No and Edit All Calls parameter to No.

15 Set the Sys Diag parameter to indicate whether an administrator can perform all system diagnostics.

With the Yes setting, an administrator can use any of the options in the Sys Diag menu by local or remote management. The default value is Yes.

No specifies that an administrator cannot use any of the options in the Sys Diag menu.

16 Set the All Port Diag parameter to indicate whether an administrator can perform all serial host port diagnostics.

With the Yes setting, an administrator can perform all the tasks listed in the Port Diag menu. The default value is Yes.

No specifies that an administrator cannot perform any of the tasks listed in the Port Diag menu.

17 Set the Own Port Diag parameter to indicate whether an administrator can perform port diagnostics for his or her own serial host port.

With the Yes setting, an administrator can use remote management to perform any of the options in the Port Diag menu for the port that has been called. The default value is Yes.

No specifies that the administrator cannot perform port diagnostics for his or her own serial host port. To disable the administrator's ability to perform diagnostics for his or her own port, set Own Port Diag parameter No and All Port Diag parameter to No.

18 Set the Download parameter to indicate whether an administrator can use the Save Cfg command to download the DSL Terminator configuration.

With the Yes setting, a user can download profiles and other configuration parameters to another device for backup. The default value is Yes.

No specifies that an administrator cannot download profiles and other configuration parameters.

Note: You cannot download passwords to another device, regardless of a Yes or No setting.

19 Set the Upload parameter to indicate whether an administrator can use the Restore Cfg command to upload the DSL Terminator configuration from another device.

– With the Yes setting, a user can upload profiles and other configuration parameters from another device to the DSL Terminator. To use the Restore Cfg command, set the Upload parameter to Yes in order to use the Restore Cfg command. The default value is Yes.

– No specifies that the user cannot upload profiles and other configuration parameters from another device to the DSL Terminator.

Note: When you save a configuration to file, passwords are not included in the download. Restoring from file clears all passwords on the DSL Terminator.

20 Set the Field Service parameter to grant or restrict privileges to perform Lucent-provided field service operations, such as uploading new system software.

Yes grants privileges. The default value is Yes.

No restricts privileges. Selecting No does not disable access to any DSL Terminator operations. Field service operations are special diagnostic routines not available through DSL Terminator menus.

21 Close the new Security profile.

Activating a Security profile

When you log into the DSL Terminator, you can only view settings because the Default profile is active. To make any changes or perform any administrative tasks, you must activate the Full Access profile or a profile that has been configured to allow setup or administrative tasks.

Activate a profile as follows:

1 Press Ctrl-D to open the DO menu.

2 Press P, or select P=Password.

3 In the list of Security profiles that opens, select the profile you want to activate.

The DSL Terminator prompts you for the password.

4 Specify the appropriate password, and press Enter.

When you enter the correct password, the DSL Terminator displays the message `Password accepted. Using new security level`. If you enter an incorrect password, the DSL Terminator prompts you again for the password.

Using the Full Access profile

The Full Access profile is the superuser profile which allows you to configure your system, reset the unit, and upgrade system software. This profile is intended to remain totally open, with all privileges set to Yes. The default password assigned to the profile is *Ascend*. A user who knows the password for the Full Access profile can perform any operation on the DSL Terminator.

Note: To prevent unauthorized access, change the default password as soon as possible.

Following are the default settings for the Full Access profile:

```
Name=Full Access
Passwd=Ascend
Operations=Yes
Edit Security=Yes
Edit System=Yes
Edit Line=Yes
Edit All Ports=Yes
Edit Own Port=N/A
Edit All Calls=Yes
Edit Com Call=N/A
Edit Own Call=N/A
Edit Cur Call=N/A
Sys Diag=Yes
All Port Diag=Yes
Own Port Diag=N/A
Download=Yes
```

```
Upload=Yes
Field Service=Yes
```

Configuring the DSL Terminator to recognize the authentication server

For the DSL Terminator unit to communicate with the authentication server, you must set the parameters in Table 2-2.

Table 2-2. Authentication server parameters

Location	Parameters with sample values
Ethernet > Mod Config > DNS	Password Host=10.0.0.1
Ethernet > Mod Config > Auth	Password Port=10 Password Server=Yes

For the parameters to work, you must meet these conditions:

- The DSL Terminator unit must request PAP-TOKEN authentication.
- You must have the APP Server utility running on a UNIX or Windows workstation on the local network.

  Ascend Password Protocol (APP) is a UDP protocol.

To configure the DSL Terminator unit to recognize the authentication server, follow these steps:

1. Open the Ethernet menu.
2. Open the Mod Config menu.
3. Open the DNS menu.
4. For the Password Host parameter, specify the IP address of the authentication server on the remote network.
5. Return to the Mod Config menu and open the Auth menu.
6. For the Password Port parameter, specify the User Datagram Protocol (UDP) port number that the server indicated by Password Host is monitoring.

   Valid port numbers range from 0 to 65535. The default value is 0 (zero). This setting indicates that the authentication server is not monitoring a UDP port.
7. Set the Password Server parameter to Yes.

   This setting specifies that callers use security-card authentication.
8. Save your changes.

Setting up user authorization

You can set up user authorizations for different types of security.

Setting up terminal-server security

A terminal-server connection is a host-to-host connection that uses Telnet. This section also applies to locally connected terminal-server users, and describes how to limit access to the terminal-server features such as Telnet server, and Rlogin server.

You can customize and limit access to the terminal-server interface in the following ways:

- Turn terminal-server operation on or off
- Restrict access to the terminal-server command line

Disconnect a user's Telnet connection by using the session ID for the connection

For complete information on setting up terminal-server connections in RADIUS, see the *TAOS RADIUS Guide and Reference*.

Turning terminal-server operation on or off

To specify whether users can access the terminal-server interface, proceed as follows:

1 Open the Ethernet > Mod Config > TServ Options menu.

2 To enable terminal-server access, set TS Enabled to Yes. To disable terminal-server access, set TS Enabled to No.

3 Save your changes.

Table 2-3. Characters used in the terminal-server prompt specification

Character combination	Description
`\n`	Carriage return/line feed
`\t`	Tab
`\\`	Displays a double backslash (\\)

Note: Any characters other than `\n` and `\t` that have a single backslash (\) in front of them are removed.

For example, you could enter

```
Welcome to\n\t\\Ascend Remote Server\\\Enter your user name:
```

to display the following on the terminal-server screen:

```
Welcome to
       \\Ascend Remote Server\\
Enter your user name:
```

4 Set Prompt Format to Yes.

This field that determines whether you are able to use the multiline format for the terminal-server prompt. With a No setting, the DSL Terminator does not interpret the line feed/carriage return character or the tab character.

5 Set the Login Timeout parameter.

This value specifies the total number of seconds that a user has to attempt a successful login. The default value is 300 seconds. The DSL Terminator disconnects a user who is unable to login completely within the specified number of seconds. Enter a value from 0 to 300 seconds. The timer begins when the login prompt appears on the terminal-server screen, and if not reset, it continues throughout the user's subsequent login attempts.

6 Save your changes.

Dealing with unauthorized Telnet and terminal-server sessions

When a user activates a Security profile, the DSL Terminator generates a Syslog message notifying you that the event occurred (if Syslog is enabled). A user can activate a Security profile in a Telnet session or a serial-line COM port session by selecting the Security profile and specifying the proper password. When a user activates a Security profile, new Syslog messages show the name of the Security profile, the IP address of the Telnet client or the COM port number, and the local IP address.

The EventSyslog message is at the notice level and it has one of the following formats:

`^DP(assword)ASCEND: "`*`profile_name`*`" ... for `*`remote_IP`*` on `*`local_IP`*

`ASCEND: "`*`profile_name`*`" ... from `*`COM_port`*` on `*`local_IP`*

Argument	Specifies
profile_name	The name of the activated Security profile.
remote_IP	The IP address of the Telnet client.
local_IP	The local IP address of the DSL Terminator.
COM_port	The COM port number for the session.

On system login, the DSL Terminator does not generate a Syslog message for the Default Security profile. But it does generate a Syslog message if the Default Security profile is accessed for anything other than system login.

The following two messages signal that a Telnet client has enabled a Security profile:

```
Jan 10 10:05:17 eng-lab-141 ASCEND: "Full Access" security profile
enabled for 206.65.212.9 on 192.168.6.141.
```

```
Jan 10 10:07:26 eng-lab-141 ASCEND: "Default" security profile enabled
for 206.65.212.23 on 192.168.6.141.
```

The following message signals that a COM port user has enabled the Full Access profile:

```
Jan 10 10:03:52 eng-lab-141 ASCEND: "Full Access" security profile
enabled from com port 0 on 192.168.6.141.
```

Enabling the RADIUS Boot server

You can configure the DSL Terminator to obtain pseudo-user configuration information from a different RADIUS server other than that used for authentication. You can specify up to two servers, with one acting as a backup if the first server fails to respond to the requests.

To enable this feature, you must configure at least one host and a port number. If a Boot server is not configured, the pseudo-user configuration information is obtained from the main RADIUS server.

The following parameters define the RADIUS hosts (shown below with sample values):

```
Ethernet > Mod Config > Auth

Auth...
Auth Boot Host #1=204.178.215.249
Auth Boot Host #2=0.0.0.0
Auth Boot Port=1812
```

Parameter	Specifies
Auth Boot Host #1	IP address of the first RADIUS server that is contacted to obtain the pseudo user configuration.
Auth Boot Host #2	IP address of a backup RADIUS server that is contacted should the first fail to reply.
Auth Boot Port	Port number used to contact the servers. The range is 1 to 65535.

To communicate with the Boot server you must set values for a Key and optionally, a Src port for the RADIUS server to use during normal authentication.

Setting up SNMP security

SNMP provides a way for computers to share networking information. SNMP recognizes two types of communicating devices: agents and managers. An agent (such as the DSL Terminator) provides networking information to a manager application running on another computer. The agents and managers share a database of information, called the Management Information Base (MIB).

A trap is a mechanism in SNMP for reporting system change in real time. To report system change, the DSL Terminator sends a traps-PDU across the Ethernet interface to the SNMP manager. A complete list specifying the events that cause the unit to send a traps-PDU appears in the Ascend Enterprise Traps MIB.

You can set up SNMP security in the following ways:

- Specify passwords for SNMP managers with access to the DSL Terminator
- Set up SNMP traps
- Restrict the hosts that can issue SNMP commands

Table 2-4 shows the parameters for protecting access to SNMP on the DSL Terminator. The values shown are examples.

Table 2-4. SNMP security parameters

Location	Parameters with sample values
Ethernet > Mod Config > SNMP Options	Read Comm=new-string R/W Comm=unique-string Security=Yes RD Mgr1=10.21.4.5 RD Mgr2=10.21.4.7 RD Mgr3=10.21.4.55 RD Mgr4=10.21.4.103 RD Mgr5=10.21.4.64 WR Mgr1=10.21.4.11 WR Mgr2=0.0.0.0 WR Mgr3=0.0.0.0 WR Mgr4=0.0.0.0 WR Mgr5=0.0.0.0
Ethernet > SNMP Traps > *any SNMP Traps profile*	Name= Alarm=Yes Port=No Security=No Comm= Dest=0.0.0.0

Password-protecting SNMP

An SNMP manager application residing on a workstation on the local or remote network can access management information, set alarm thresholds, and change some settings on the DSL Terminator. To password protect this type of network access, you must assign the Read and Read/Write SNMP community strings. To assign Read and Read/Write SNMP community strings, proceed as follows:

1 Open the Ethernet > Mod Config > SNMP Options menu.

2 Set the Read Comm parameter to specify the Read community string.

This string authenticates an SNMP manager accessing the DSL Terminator to perform read commands, that is, the Get and Get Next commands. The Get command requests information. The Get Next command enables an SNMP manager to obtain a table of information, such as a routing table. After you enter a string for the Read Comm parameter, users must supply it to use the Get and Get Next commands.

3 Set the R/W Comm parameter to specify the Read/Write community string.

This string authenticates an SNMP manager accessing the DSL Terminator to perform read and write commands, that is, the Get, Get Next, and Set commands. The Set command enables an SNMP manager to change information maintained by the DSL Terminator. After you enter a string for the R/W Comm parameter, users must supply it to use the Get, Get Next, and Set commands. You can use the original SNMPv1 definition of the community string (a string of octets that is compared to a similar string in the receiving SNMP entity). If the string in the packet received exactly matches a community string in the receiving entity, the packet is considered “authentic.”

The defaults for SNMP v1 (without authentication) are:

Ethernet > Mod Config > SNMP Options > Read Comm=public

Ethernet > Mod Config > SNMP Options > R/W Comm=write

If you wish to use SNMP authentication, you use a new version of the Read/Write community string:

`Ethernet > Mod_config > SNMP Options > R/W Comm=`***`name`***`|`***`secretkey`***

where:

- ***`name`*** is the name you want to assign to the read-write community name.
- ***`secretkey`*** is the alphanumeric key used for authentication.
- | (vertical bar/pipe) separates the ***`name`*** from the ***`secretkey`***.

This setting causes the DSL Terminator to require SNMP SET REQUEST packets to be authenticated, with *`secretkey`* as the shared (but not transmitted) secret.

The data, time, and hash values are transmitted with the packet, enabling the management station and DSL Terminator to verify that the packet has been produced by an authorized system and that the packet not been altered or significantly delayed in transmission.

The MD5 hash guarantees a high likelihood that only a system that knows the secret authentication key has generated the packet, while the time variables guarantee a high likelihood that an attacker did not collect an authenticated packet and transmit it at a time of its own choosing (after a significant delay).

Note: You cannot turn SNMP write off, so you must set a secret R/W Comm string. The default R/W Comm string is `write`. Anyone who has used an Lucent product probably knows this default string, so it does not provide any real security.

4. If you are using authenticated SNMP, configure the SNMP management station to communicate with a DSL Terminator through authenticated SNMP (as described in "Configuring the SNMP manager to use SNMP authentication").
5. Save your changes.

Configuring the SNMP manager to use SNMP authentication

To communicate with a DSL Terminator that has been configured to use authenticated SNMP, an SNMP management station must construct an SNMP packet in the new format for the Read/Write community string, including the secret key:

`name`|*`secretkey`*

If you configure the unit to use authenticated SNMP, it does not accept packets from an SNMP management station that uses the string format without the vertical bar/pipe.

Setting up SNMP traps

To configure parameters related to SNMP traps security, proceed as follows:

1. Open the Ethernet > SNMP Traps menu.
2. Open a blank SNMP Traps profile.
3. For the Name parameter, specify the SNMP manager to which the DSL Terminator sends traps-PDUs.

   You can specify up to 31 characters. The default value is null. The value you specify becomes the name of the profile.

4 Set the Alarm parameter to specify whether the DSL Terminator sends a traps-PDU to the SNMP manager when an alarm event occurs.

Alarm events are defined in RFC 1215 and include the following:

- coldStart—The unit started up from a power-off condition.
- warmStart—The unit started up from a power-on condition, typically by a system reset.
- linkDown—A WAN link or Ethernet interface has gone offline.
- linkUp—A WAN link or Ethernet interface has come online.

You can specify either Yes or No for the Alarm parameter. Yes specifies that the unit traps alarm events. No specifies that the unit does not trap alarm events. The default value is Yes.

5 Set the Port parameter to specify whether the DSL Terminator traps serial host port state changes and sends traps-PDUs to the SNMP manager.

The unit can record the following serial host port events:

- portInactive
- portDualDelay
- portWaitSerial
- portHaveSerial
- portRinging
- portCollectDigits
- portWaiting
- portConnected
- portCarrier
- portLoopback
- portAcrPending
- portDteNotReady

You can specify either Yes or No for the Port parameter. Yes specifies that the DSL Terminator traps serial host port state changes. No specifies that the DSL Terminator ignores serial host port state changes. The default value is No.

6 Set the Security parameter to specify whether the DSL Terminator traps these events:

- authenticationFailure—Occurs when authentication has failed. For a full explanation of this event, see RFC-1215.
- consoleStateChange—Occurs when a VT100, Palmtop, or Telnet port changes its state.
- portUseExceeded—Occurs when the port exceeds the maximum number of DS0 minutes set by the DSL Terminator DS0 Mins parameter in the Port profile.
- systemUseExceeded—Occurs when the DSL Terminator exceeds the maximum number of DS0 minutes set by the DSL Terminator DS0 Mins parameter in the System profile.

You can specify either Yes or No for the Security parameter. Yes specifies that the DSL Terminator traps the events. No specifies that the DSL Terminator does not trap the events. The default value is No.

7 Set the Comm parameter to specify a community name.

The string you specify becomes a password that the DSL Terminator sends to the SNMP manager when an SNMP trap event occurs. The password authenticates the sender identified by the IP address in the IP Adrs parameter.

For the community name, you can enter an alphanumeric string of up to 31 characters. The default value is null. To turn off SNMP traps, leave the Comm parameter blank and set Dest to 0.0.0.0.

8 Set the Dest parameter to specify the IP address of the SNMP manager to which the DSL Terminator sends traps-PDUs.

Specify an IP address in dotted decimal notation. An IP address consists of four numbers from 0 to 255, separated by periods. If a subnet mask is in use, you must specify it. Separate a subnet mask from the IP address with a slash. The default value is 0.0.0.0/0.

The DSL Terminator ignores any digits in the IP address hidden by a subnet mask. For example, the address 200.207.23.1/24 becomes 200.207.23.0. To specify a route to a specific host, use a mask of 32.

The Dest parameter does not apply if the DSL Terminator does not support IP (the Route IP parameter is set to No) or if Combinet encapsulation is in use (the Encaps parameter is set to COMB).

9 Save your changes.

Restricting the hosts that can issue SNMP commands

The DSL Terminator is an SNMP-enabled device that supports a variety of MIBs. For large networks, you should specify which stations can use SNMP manager applications to initiate read or read/write access to those MIBs.

You can specify up to five IP hosts that can read traps and other information from the DSL Terminator, and five hosts that can access MIB read-write access. The unit checks the version and community strings before making source IP address comparisons.

To restrict the hosts that can issue SNMP commands, proceed as follows:

1 Open the Ethernet > Mod Config > SNMP Options menu.

2 Make sure that the Security parameter is set to Yes.

This parameter specifies that the DSL Terminator must compare the source IP address of packets containing SNMP commands against a list of qualified IP addresses.

3 Specify the IP addresses of hosts that have SNMP read permission.

For example, you might enter the following settings:

```
RD Mgr1=10.1.2.3
RD Mgr2=10.1.2.4
RD Mgr3=10.1.2.5
RD Mgr4=10.1.2.6
RD Mgr5=10.1.2.7
```

If the Security parameter is set to Yes, only SNMP managers at the specified IP addresses can execute the SNMP Get and Get Next commands.

4 Specify the IP addresses of hosts that have SNMP write permission.

For example, you might enter the following settings:

```
WR Mgr1=10.9.8.1
WR Mgr2=10.9.8.2
WR Mgr3=10.9.8.3
WR Mgr4=10.9.8.4
WR Mgr5=10.9.8.5
```

If the Security parameter is set to Yes, only SNMP managers at the specified IP addresses can execute the SNMP Get, Get Next, and Set commands.

5 Save your changes.

Using SNMP to specify the primary RADIUS server

By default, if the DSL Terminator unit uses a secondary RADIUS authentication server because the primary one goes out of service, the DSL Terminator unit does not use the first host until the second machine fails. This situation occurs even if the first host has come online while the second host is still servicing requests. However, you can use an SNMP set command to specify that the DSL Terminator unit use the first host again. Such a need might arise if you shut down the primary server for service and then make it available again.

Every time you reset the server using the set command, the DSL Terminator unit generates an SNMP trap. The DSL Terminator unit also generates a trap if it changes to the next server because the current server fails to respond. The trap is an Enterprise Specific Trap (18) and is accompanied by the Object ID and IP address for the new server. The Object ID for Authentication Server is 1.3.6.1.4.1.529.13.3.1.11.*x.* where *x* is the index of the current server (1–3).

For details, see the Ascend Enterprise MIB. You can download the most up-to-date version of the Ascend Enterprise MIB by logging in as `anonymous` to ftp.ascend.com. (No password is required.)

Setting up a Domain Name System (DNS)

DNS is a TCP/IP service that enables you to specify a symbolic name instead of an IP address. A symbolic name consists of a username and a domain name using the format *`username@domain name`*. The username corresponds to the host number in the IP address; the domain name corresponds to the network number in the IP address. A symbolic name might be `steve@abc.com` or `joanne@xyz.edu`.

DNS maintains a database of network numbers and corresponding domain names on a domain name server. When you use a symbolic name, DNS translates the domain name into an IP address, and sends it over the network. When the Internet service provider receives the message, it uses its own database to look up the username corresponding to the host number.

You can set up two types of DNS configurations:

- Global l DNS, in which you specify the DNS server(s) known to all DSL Terminator users on connected local interfaces.
- Client DNS, in which you specify the DNS server(s) known to DSL Terminator users for which a specify Connection profile has been applied.

Table 2-5 lists the parameters you can set.

Table 2-5. DNS parameters

Location	Parameters with sample values
Ethernet > Mod Config > DNS	Domain Name=abc.com Sec Domain Name=xyz.com Pri DNS=10.2.3.56/24 Sec DNS=10.2.3.107/24 List Attempt=No List Size=6 Client Pri DNS=101.10.10.1 Client Sec DNS=101.10.10.2 Allow as Client DNS=Yes Sec Domain Name=xyz.com
Ethernet > Connections > a*ny Connection profile* > IP Options	Client Pri DNS Client Sec DNS

Setting global DNS parameters

To set global DNS parameters, proceed as follows:

1 Open the Ethernet > Mod Config > DNS menu.

2 Set the Domain Name parameter to specify a primary domain name to use for lookups.

The unit searches for the DNS Server(s) in the Domain Name parameter first, and then in the domain specified in the Sec Domain Name parameter.

3 Set the Sec Domain Name parameter to specify a secondary domain name to use for lookups.

4 Set the Pri DNS parameter to specify the IP address of the primary domain name server for use on connected local interfaces.

The address consists of four numbers from 0 to 255, separated by periods. The default value is 0.0.0.0. Accept this default if you do not have a domain name server.

5 Set the Sec DNS parameter to specify the IP address of the secondary domain name server for use on connected local interfaces.

The address consists of four numbers from 0 to 255, separated by periods. The default value is 0.0.0.0. Accept this default if you do not have a secondary domain name server.

The DSL Terminator uses the secondary server only if the primary one is inaccessible. The Sec DNS parameter applies only to Telnet connections running under the unit's terminal-server interface.

6 Set List Attempt to Yes.

DNS can return multiple addresses for a hostname in response to a DNS query, but it does not include information about availability of those hosts. A user typically attempts to access the first address in the list. If that host is unavailable, the user must try the next host, and so forth. However, if the access attempt occurs automatically as part of immediate services, the physical connection is torn down when the initial connection fails.

The DNS List Attempt feature helps the DSL Terminator avoid tearing down physical links. The user can try one entry in the DNS list of hosts when logging in through Telnet

from the terminal server or immediate Telnet, and, if that connection fails, the user can try each succeeding entry.

You can specify one of the following settings:

– Yes specifies that the DSL Terminator enables a user to try the next host in the DNS list if the first Telnet login attempt fails.

– No turns off the List Attempt feature. The default value is No.

7 If you set List Attempt to Yes, set the List Size parameter.

8 The List Size parameter specifies the maximum number of hosts the DSL Terminator can list in response to a DNS query. Specify a number from 0 to 35. The default value is 6.

Setting client DNS parameters

To set up client DNS in which connection-specific DNS parameters are applied, proceed as follows:

1 Open the Ethernet > Connections menu.

2 Open a Connection profile

3 Open the IP Options menu.

4 Set the Client Pri DNS parameter.

5 Set the Client Sec DNS parameter.

The default value is 0.0.0.0. Accept this default if you do not have a secondary client DNS server.

6 Set the Allow As Client DNS parameter to Yes or No.

– Yes enables WAN clients to use local DNS servers.

– No disables WAN clients from using local DNS servers.

No is the default.

Example of DNS configuration

This sample shows how to specify two local DNS servers and enable the DNS list feature.

1 Open the Ethernet > Mod Config > DNS menu.

2 Specify your domain name.

3 Specify the IP addresses of a primary and secondary DNS server, and turn on the DNS list attempt feature. For example:

```
Mod Config
    DNS…
        Domain Name=abc.com
        Pri DNS=10.2.3.56/24
        Sec DNS=10.2.3.107/24
        List Attempt=Yes
```

4 Save your changes.

Disabling remote management access

To prevent an administrator from accessing the DSL Terminator from a remote unit by means of AIM or MP+ remote management, set System > Sys Config > Remote Mgmt to No. Proceed as follows:

1. Open the System > Sys Config menu.
2. Set Remote Mgmt to No.
3. Exit and save your changes.

For related information about remote management, see “Using remote management to configure far-end units” on page 1-3.

Password-protecting Telnet access

You can assign a Telnet password to restrict administrators from accessing the DSL Terminator across the network from a remote PC running Telnet. Proceed as follows:

1. Open the Ethernet > Mod Config menu.
2. Set the Telnet PW parameter.

   Specify up to 20 characters. Any user who initiates an incoming Telnet session to the DSL Terminator must supply this password before the Telnet session is established.

   If a user initiates the Telnet session from the WAN, the connection must first be authenticated as specified in a Connection profile.
3. Set the Telnet Security parameter to specify whether or not you allow a single authentication process when users initiate a telnet session.
4. Save your changes.

Limiting access to services and protocols

To limit the services and protocols that a link can use, you must specify a value for each of the attributes listed in Table 2-6. If you do not specify a value, the DSL Terminator unit does not restrict the services and protocols the link can use.

Table 2-6. Limiting services and protocols

Attribute	Description	Possible values
Framed-Protocol (7)	Specifies the type of protocol the link can use.	PPP (1) MPP (256) FR (261) FR-CIR (263) ATM-1483 ATM-FR-CIR By default, the DSL Terminator unit does not restrict the type of protocol a link can use.

Table 2-6. Limiting services and protocols (continued)

Attribute	Description	Possible values
Password (2)	Specifies the user's password.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Name (1)	Specifies the user's name.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Service (6)	Indicates the type of framed services the link can use.	Framed-User (2) Dialout-Framed-User (5) By default, the DSL Terminator unit does not restrict the framed services that a link can use.

To limit access to services and protocols for a connection, follow these steps:

1. On the first line of the profile, specify the User-Name and Password attributes.
2. Set the User-Service attribute to Framed-User.
3. To specify the type of framed protocol the link can use, set the Framed-Protocol attribute. When you set this attribute, the DSL Terminator unit does not allow any other type of framed protocol.

   What Framed-Protocol does depends on how you set User-Service:

   If User-Service=Framed-User or is unspecified, a host requesting access can dial in using the framing specified by Framed-Protocol. The DSL Terminator unit rejects other types of framing.

   A host requesting access can also dial in without using a framed protocol, but can then change to the framing specified by the Framed-Protocol attribute.

   If User-Service=Framed-User or is unspecified, and Framed-Protocol has no specified value, the administrator can use any framed protocol.

The dial-in host in this example can use only PPP protocols (PPP, MP+, or MP).

```
Lucent Password="SDSLPipe", User-Service=Framed-User
       Framed-Protocol=PPP,
       Framed-Address=200.250.55.9,
       Framed-Netmask=255.255.255.248,
       Ascend-Link-Compression=Link-Comp-Stac,
       Ascend-Route-IP=Route-IP-Yes,
       Ascend-Metric=2
```

Configuring WAN Access

3

Introduction to WAN configuration 3-1
Configuring DS3-ATM connections 3-3
Configuring UDS3 connections and lines 3-6
Configuring the OC3-ATM connections 3-7
Configuring T1 lines 3-15
Configuring E1 lines 3-18

Introduction to WAN configuration

The has two expansion slots that can support cards which provide switching or routing between ATM and Frame Relay networks.

Menus and profiles

To configure the DSL Terminator, you set parameters in the VT100 menus. For a description of navigating the interface, see the *DSL Terminator Hardware Installation Guide*. Many of the menus and submenus include profiles, which are groups of related parameters.

How the VT100 menus relate to slots and ports

The numbers in the VT100 menus relate to slot numbers in the DSL Terminator, which can represent actual expansion slots or *virtual* slots on the unit's motherboard.

System slot

The system itself is assigned slot number 0 (menu 00-000). The System menu contains the following profiles and submenus that are all related to systemwide configuration and maintenance:

```
00-000 System
   00-100 Sys Config
   00-200 Sys Diag
   00-300 Security
   00-400 Destinations
```

WAN slots

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

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

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


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



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

Following is an example of a T1 or E1 menu:

```
10-000 Net/8T1 (or Net/8E1)
   10-100 Line Config
      any profile
             Name=
             Line 1...
                Enabled=Yes
                Nailed Group=0
```

```
                Framing Mode=ESF
                Front End=CSU
                Encoding=B8ZS
                Length=N/A
                Buildout=0 dB
                Clock Source=Yes
                First DS0 channel=1
                 Last DS0 channel=24
              Line 8...

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

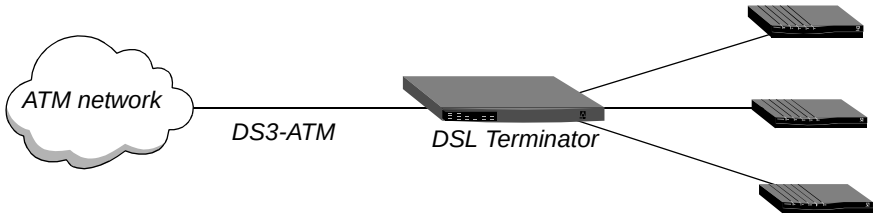
Ethernet and WAN slots

Slot 3 is the Ethernet slot (menu 30-000). The Ethernet menu contains submenus and profiles related to the local network, routing and bridging, and WAN connections.

Configuring DS3-ATM connections

The DSL Terminator DS3-ATM card is a 44.736 Mbps communications circuit that can be used to either route ATM traffic or perform Layer 2 switching between Asynchronous Transfer Mode (ATM) and Frame Relay networks. Figure 3-1 shows a sample DS3-ATM setup.

Figure 3-1. Example of an DS3-ATM setup



You can configure two different types of connections for the DS3-ATM card, a routed connection that uses ATM-encapsulation, or a switched connection between ATM and Frame Relay networks.

The following list summarizes the capabilities of the DS3-ATM card:

- One unchannelized DS3 port with integrated CSU/DSU
- Layer 3 routing between ATM networks
- Layer 2 PVC switching between ATM and Frame Relay networks
- Support for RFC 1483 (Multiprotocol Encapsulation over ATM Adaptation Layer 5)
- Protocol conversion between ATM (RFC 1483) and Frame Relay (RFC 1490) data

- ATM Forum UNI 3.1 support
- Operations, Administration and Maintenance (OAM) F4/F5 support
- No interim link management interface (ILMI) support

Configuring DS3-ATM lines

Currently, the DS3-ATM card only supports C-Bit-PLCP framing and static activation. You must, however, enable the line, specify the length of the cables connecting the card to the WAN interface, and specify a nailed group. The unit uses the nailed group to route traffic between physical interfaces.

The Name parameter (displayed after the line's physical address in the Dir command output) enables you to optionally assign the profile a name of up to 16 characters.

By default each DS3-ATM line is disabled. When the DS3 interface is disabled, it transmits the DS3 Idle Signal to the far end.

To assign the line a name and enable it, proceed as in the following example:

1 Open Net/DS3-ATM > Line Config > *any slot profile*:

```
Net/DS3-ATM
   Line Config
     any slot profile
          Name=
          Enabled=Yes
          Nailed-group=1
          TrnkGrp=0
          Line 1...
```

2 Specify a name:

```
Name=atm-la
```

3 Set Enabled to Yes:

```
Enabled=Yes
```

4 If the DS3 line cable length is longer than 255 feet, open the Line 1 subprofile and set the Long cable (>256ft) parameter to Yes. Otherwise, leave it at its default value.

```
Line 1...
  Activation=Static
  Cell payload scramble=Yes
  Framer mode=C-bit PLCP
  Loopback=None
  Long cable (>256ft)=Yes
 Vpi/Vci range=0-15/32
```

ATM cell payload scrambling is enabled by default. Disable it only if the far end switch has disabled the corresponding functions.

5 Set the Vpi/Vci range to one of the following values (provided by your network service provider):

```
0-1/32-32768
0-3/32-16383
0-7/32-8191
```

```
0-15/32-4095
0-31/32-2047
0-63/32-1023
0-127/32-511
0-255/32-255
```

The default is `0-15/32-4095`

6 Save and exit the DS3-ATM profile.

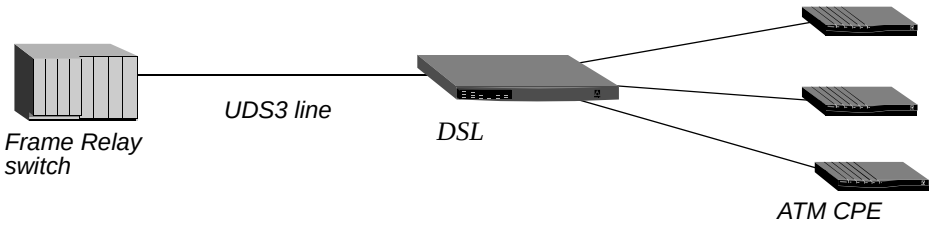
Configuring IP over ATM

You can set up an IP-routed connection between an ATM customer premise equipment (CPE) and an ATM network. To configure this connection, you must perform the following general steps:

- Activate the DS3-ATM card and specify a nailed group. The DSL Terminator uses the nailed group to route traffic received on an interface to the DS3-ATM card.
- Configure a Connection profile on the DSL Terminator for the remote ATM device. This connection profile must specify the type of ATM encapsulation, the Virtual Path Identifier (VPI) and Virtual Channel Identifiers (VCI) as defined by the ATM service provider, and the nailed group configured in the profile for the DS3-ATM card.

Figure 3-2 illustrates an example IP over ATM.

Figure 3-2. IP over ATM



Configuring the ATM card

To configure the ATM card, proceed as in the following example:

1 Open Net/DS3-ATM > Line Config > *any slot profile*:

```
Net/DS3-ATM
  Line Config
   any slot profile
     Name=
     Enabled=Yes
     Nailed-group=1
     TrnkGrp=0
     Line 1...
```

2 Specify a name:

`Name=atm-sf`

3 Set Enabled to Yes

`Enabled=Yes`

4 Specify a nailed group:

```
Nailed-group=5
```

5 Save and exit the DS3-ATM profile.

Configuring the Connection profile for the remote device

To configure the Connection profile, proceed as in the following example:

1 Open a Connection profile.

2 Specify the name of the remote device and activate the profile. For example:

```
Ethernet
   Connections
      Station=atm-cpe
      Active=Yes
```

Note: Make sure that you specify the Station name exactly, including case changes.

3 Specify ATM encapsulation:

```
Encaps=ATM
```

4 Specify the ATM VPI/VCI for the remote device. Your ATM service provider should give you these values:

```
Encaps options...
  vpi=12
  vci=42
  Circuit=N/A
```

5 Specify the IP address of the remote device:

```
Ip options...
  LAN Adrs=192.168.2.1
  ...
  ...
```

6 Specify the call-type:

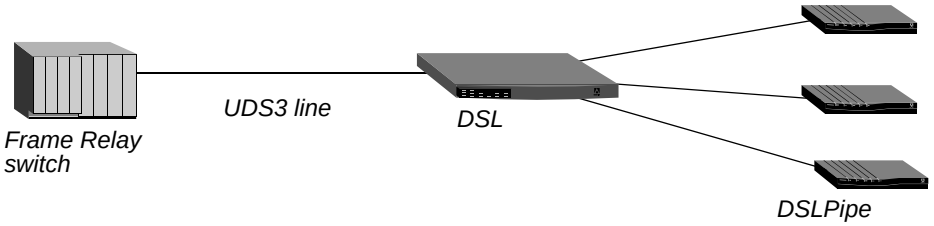
```
Telco options...
  Call Type=Nailed
  ..
  ..
```

7 Close the Connection profile

Configuring UDS3 connections and lines

The DSL Terminator unchannelized DS card (UDS3) is a 44.736 Mbps communications circuit that can be used to concentrate incoming traffic and direct it to a Frame Relay switch. Figure 3-3 shows an example UDS3 setup.

Figure 3-3. Example UDS3 setup



The UDS3 card provides support for the following:

- One Frame Relay link, possibly containing multiple Data Link Connection Indicators (DLCIs), can be active per line
- IP routing
- Layer 2 Frame Relay switching
- The DS3 MIB (RFC 1407)

In a UDS3 profile, the Name parameter enables you to assign the profile a name of up to 16 characters. It is displayed after the line's physical address in the Dir command output.

By default, each UDS3 line is disabled. When the DS3 interface is disabled, it transmits the DS3 Idle Signal to the far end. The UDS3 card only supports C-Bit-Parity framing and B3ZS encoding.

To assign the UDS3 line a name and enable it, proceed as in the following example:

1 Open Net/UDS3 > Line Config > *any slot profile*:

```
Net/UDS3
  Line Config
   any slot profile
     Name=
     Enabled=Yes
     Nailed-group=1
     TrnkGrp=0
    Line 1...
```

2 Specify a name:

```
Name=uds3-sf
```

3 Set Enabled to yes.

```
Enabled=Yes
```

4 Specify a nailed group:

```
Nailed-group=5
```

5 Save and exit the UDS3 profile.

Configuring the OC3-ATM connections

The following list summarizes the capabilities of the OC3-ATM card:

- One unchannelized STS-3c/STS-1 OC3 port
- Fiber SC-1 or copper RJ45 physical interface, single mode
- Support for RFC 1483 (Multiprotocol Encapsulation over ATM Adaptation Layer 5)

- Support for RFC 2364 (PPP over ATM AAL5)
- ATM Forum UNI 3.1 support
- Operations, Administration and Maintenance (OAM) F4/F5 support
- No interim link management interface (ILMI) support

Table 3-1 lists the sections describing common tasks you might have to perform to configure the OC3-ATM card. The table includes a brief description of each task, and lists the parameters you will use.

For complete information about the associated parameters, see the *DSL Terminator Reference*.

Table 3-1. OC3-ATM line configuration tasks

Task	Description of task	Associated parameters
Configuring the OC3-ATM lines	Configure the OC3 physical line, including activating the line, specifying its signaling, assigning it to a nailed group, and specifying whether the transmit or receive.	Enable Framer Rate Nailed-Group Loop-Timing Name Rx Descramble Disabled Tx Scramble Disabled Rx Pyld Dscrmb Disabled Tx Pyld Scrmb Disabled
Specifying the VPI-VCI Range	You can select the best combination of VPI and VCI bit sizes to fit the list of supported VPI/VCI pairs obtained from the network provider.	VPI/VCI Range
Following are the possible ranges and their relevant bit sizes:	Provides examples of how to configure an IP over ATM routed connection and a switched ATM-to-Frame Relay connection.	N/A

Net/OC3-SMF-ATM (Net/OC3-UTP-ATM) profile

When the DSL Terminator first detects the presence of an OC3-ATM card, it creates a default Net/OC3-SMF-ATM profile (for a fiber interface card) or a Net/OC3-UTP-ATM profile (for an unshielded twisted pair card). Both profiles contain the same parameters and are configured identically.

The following example shows the parameters in an Net/OC3-SMF-ATM profile, with the default settings:

```
10-1** Factory
  Line 1...
   >Loopback=Local
    Framer Rate=STS-3c
    Rx Descramble Disabled=No
    Tx Scramble Disabled=No
    Rx Pyld Dscrmb Disabled=No
    Tx Pyld Scrmb Disabled=No
```

```
Loop Timing=No
Vpi/Vci range=0-15/32-4095
```

Configuring the OC3-ATM lines

To configure the OC3 physical interface, you must enable the line and specify the framing it uses. You can optionally assign a name to the interface using the Name parameter.

The OC3-ATM card supports STS-3c and STS-1 signaling. By default, each OC3-ATM line is disabled. When the OC3 interface is disabled, it transmits the OC3 Idle Signal to the far end.

To configure the OC3 interface, proceed as in the following example:

1 Open the Net/OC3-SMF-ATM profile:

```
10-000 Net/OC3-SMF-ATM
  10-100 Line Config
  10-200 Line Diag
```

2 Assign the OC3 line a name, if desired:

```
Name=atm-la
```

3 Enable the line:

```
Enabled=Yes
```

4 Assign a nailed group number:

```
Nailed group=5
```

The DSL Terminator uses the nailed group to route traffic received on an interface to the OC3 card.

5 Specify the framing:

```
Framer Rate=STS-3C
```

6 For most applications, leave the Tx scrambling and Rx descrambling parameters at their default values (enabled). If the Tx scrambling parameter is enabled on the OC3 card, then the Rx descrambling parameter must be enabled at the other end (which might be an ATM switch such as the CBX).

```
Rx Descramble Disabled=No
Tx Scramble Disabled=No
Rx Pyld Dscrmb Disabled=No
Tx Pyld Scrmb Disabled=No
```

7 To specify that the OC3 card receives its clock from the WAN, leave Loop Timing at the default value of Yes. To specify that the OC3 card generates its own clock, set Loop Timing to No.

```
Loop Timing=Yes
```

8 Specify VPI-VCI range for the OC3 card. These values depend on the settings provided by your network service provider:

```
Vpi/Vci range=0-15/32-4095
```

(For more information about VPI/VCI ranges, see “Specifying the VPI-VCI Range” on page 3-10.)

9 Exit and save the profile.

Specifying the VPI-VCI Range

You can select the best combination of VPI and VCI bit sizes to fit the list of supported Virtual Path Identifier-Virtual Channel Identifier (VPI-VCI) pairs obtained from the network provider. The new values take effect as soon as you save the Net/OC3-SMF-ATM profile.

Use the VPI/VCI Range parameter to specify the VPI-VCI pair. The default setting of 0-15/32-4095 is the range of values that can be represented in a 4-bit VPI and 12-bit VCI.

Following are the possible ranges and their relevant bit sizes:

Range	# Of VPI bits	# Of VCI bits
0-1/32-32767	1	15
0-3/32-16383	2	14
0-7/32-8191	3	13
0-15/32-4095	4	12
0-31/32-2047	5	11
0-63/32-1023	6	10
0-127/32-511	7	9
0-255/32-255	8	8

Example of an IP over OC3-ATM configuration

This section provides an example of configuring an IP-routed connection that uses ATM encapsulation.

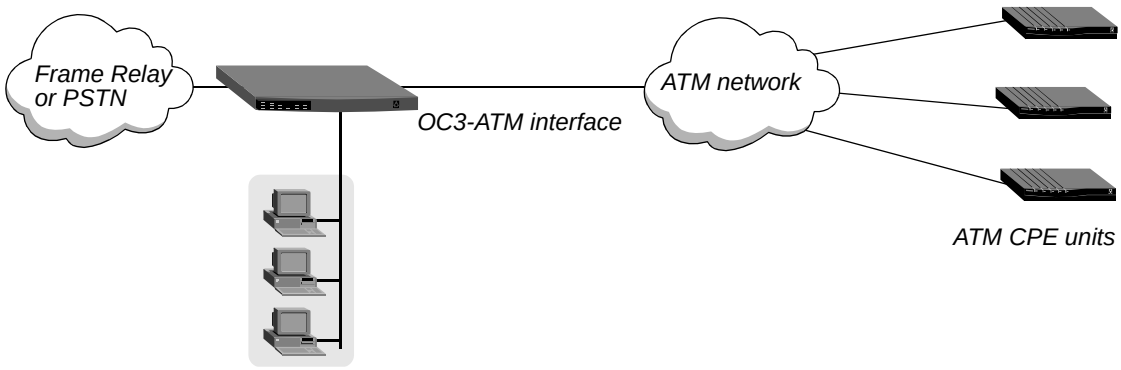
Configuring an IP-over-ATM PVC connection

You can set up an IP-over-ATM PVC connection between an ATM CPE and an ATM network. To configure this connection, you must perform the following general steps:

- Activate the OC3-ATM card and specify a nailed group. The DSL Terminator uses the nailed group to route traffic received on an interface to the OC3-ATM card.
- Configure a Connection profile on the DSL Terminator for the remote ATM device. This connection profile must specify ATM encapsulation, the Virtual Path Identifier (VPI) and Virtual Channel Identifiers (VCIs) as defined by the ATM service provider, and the nailed group configured in the OC3-ATM profile.

Figure 3-4 illustrates an example DSL Terminator IP over ATM PVC connection.

Figure 3-4. IP over ATM PVC connection



Configuring the ATM card

To configure the ATM card, proceed as in the following example:

1. Open the OC3-ATM profile.
2. Assign a name to the line, if desired:

   `Name=atm-sf`
3. Activate the line:

   `Enabled=Yes`
4. Assign a nailed group:

   `Nailed-group=5`
5. Specify the framing:

   `Framer Rate=STS-3c`
6. Verify that Loop-Timing is set to its default value of Yes:

   `Loop Timing=Yes`
7. Exit and save the profile.

Configuring the Connection profile for the remote device

To configure the Connection profile, proceed as in the following example:

1. Open a Connection profile.
2. Activate the profile:

   `Active=Yes`
3. Specify ATM encapsulation:

   `Encaps=ATM`
4. Open the Encaps submenu:
5. Specify the ATM VPI/VCI for the remote device. Your ATM service provider should give you these values:

```
vpi=12
vci=42
```

6 Open the IP Options submenu.

7 Specify the IP address of the remote device:

```
LAN Adrs=192.168.2.1
```

8 Open the Telco Options submenu.

9 Specify the call-type:

```
Call Type=Nailed
```

10 Specify the same nailed group number you specified in the Net/OC3-SMF-ATM profile:

```
Group=5
```

11 Exit and save the profile.

Traffic shaping for ATM cards

Traffic shaping enables you to control the data transmission rate of ATM cells. Traffic shaping is enabled on the DSL Terminator DS3-ATM and the OC3-ATM cards.

To configure traffic shaping on the DSL Terminator, first, configure a Traffic Shaper profile, then specify the number of the traffic shaper in a Connection profile.

Default Traffic Shaper profile

You can either create a custom Traffic Shaper profile or use the default profile (profile 16), which contains the following settings:

- Priority—15
- Bit Rate—Maximum line rate for the card. For a DS3-ATM card the maximum is 37290; for the OC3-ATM card the maximum rate is 135631.
- Peak Rate—Maximum line rate for the card.
- Max Burst Size—255
- Aggregate—No

You can not edit the default profile.

Configuring traffic shaping

This example assumes you have already configured the DS3 or OC3 line. For detailed descriptions of the parameters used to configure traffic shaping, see “Understanding traffic shaping parameters” on page 3-14.

To configure a Traffic Shaper profile:

1 Open Net/OC3-ATM (or Net/DS3-ATM)> Line Config > *any line profile*:

```
Name=Factory
Enabled=No
Nailed-group=1
TrnkGrp=9
Line 1...
```

```
Incoming VCCs...
Traffic Shapers...
```

2 Open the Traffic Shapers submenu:

```
10-1** Factory
Traffic Shapers...
 >Traffic Shaper 01
  Traffic Shaper 02
  Traffic Shaper 03
  Traffic Shaper 04
  Traffic Shaper 05
  ...
  ...
```

3 Open a Traffic Shapers profile:

```
Traffic Shapers 01
>Enabled = No
Bit Rate=1000
Peak Rate=1000
Max Burst Size=2
Aggregate=No
Priority=0
```

4 Enable the profile:

```
Enabled=Yes
```

5 Specify a bit rate (in Kilobits per second). For example:

```
Bit Rate= 2000
```

This value specifies the average bit rate at which the virtual circuit associated with this shaper transmits data.

6 Specify a peak bit rate (in Kilobits per second). For example:

```
Peak Rate= 4000
```

This value specifies the peak bit rate at which the virtual circuit associated with this shaper transmits data.

7 Specify a maximum burst size. For example:

```
Max burst size= 48
```

Max Burst Size specifies the maximum number of ATM cells (between 2 and 255) that the virtual circuit associated with this shaper can transmit to the network at the peak rate.

8 Specify how the DSL Terminator determines the bit rate of individual VCs sharing a single traffic shaper. For example:

```
Aggregate= Yes
```

With this setting, the throughput of each VC using the shaper will be the value of Bit Rate/(*number of virtual connections*). (For a description of the Aggregate parameter, see “Understanding traffic shaping parameters” on page 3-14.)

9 Specify a priority for the traffic using this traffic shaper. For example:

```
Priority=3
```

0 (zero) is the highest priority; 15 is the lowest.

10 Exit and save the profile.

11 Next, open a Connection profile that you want to use this Traffic Shaper profile. For example:

```
DSLTERM
   Station=DSL Terminator2
   Active=Yes
   Encaps=ATM
   ...
   ...
   Session options
```

12 Open the Session Options submenu.

13 Specify the number of the Traffic Shaper profile you want to use for this connection. For example:

```
Traffic shaper=12
```

14 Exit and save the profile.

15 Restart the session in order for the VC to use the new Traffic Shaper profile as follows.

16 Press Control-D to bring up the DO menu:

```
0=Esc
2=Hangup
P=Password
S=Save
C=Close Telnet
E=Termserv
D=Diagnostic
```

17 Select `2=Hangup` to end the session.
When the session is re-established, it will use the specified Traffic Shaper profile.

Understanding traffic shaping parameters

This section describes the parameters in the DSL Terminator user interface that are used to support traffic shaping. You can configure these parameters in *any OC3 or DS3 card* > Config > *any line profile* > Traffic Shapers.

Parameter	Description
Aggregate	Specifies how the DSL Terminator determines the bit rate of individual VCs sharing a single traffic shaper. 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*). The Traffic Shaper profile must be enabled for Aggregate to apply.

Parameter	Description
Bit Rate	Specifies the average bit rate (in kbps) at which the virtual circuit using a Traffic Shaping profile transmits data. 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. The Traffic Shaper profile must be enabled for Bit Rate to apply.
Enabled	Enables a Traffic Shaper profile. Specify one of the following values: • No (the default)—disables the Traffic Shaper profile • Yes—the Traffic Shaper profile is enabled
Max Burst Size	Specifies the maximum number of ATM cells the virtual circuit using a Traffic Shaping profile can transmit to the network at the peak rate. Specify a number between 2 and 255. The default value is 2. The Traffic Shaper profile must be enabled for Max Burst Size to apply.
Peak Rate	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. Specify a value (in kbps) from 0 (zero) to the maximum rate the interface supports. The maximum value for a DS3-ATM card is 37290 and 135631 for the OC3-ATM card. The default value is 1000. The Traffic Shaper profile must be enabled for Peak Rate to apply.
Priority	Specifies the priority assigned to a Traffic Shaper profile. The DSL Terminator transmits cells using a higher priority Traffic Shaper profile before it transmits cells using a lower priority Traffic Shaper profile. Specify a number between 0 and 15. The default value is 1. The Traffic Shaper profile must be enabled for Priority to apply.
Traffic Shaper	Specifies the Traffic Shaper to be used for a 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. Specify a number between 1 and 16. The default value 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 “Default Traffic Shaper profile” on page 3-12.You must re-establish the session for changes to the Traffic Shaper parameter to take effect.

Configuring T1 lines

DSL Terminator T1 connections are not channelized, but you can configure it like a T1 with any number of DS0 channels, up to 24, as specified by your carrier. With a nailed T1 line, you must manually configure some port information. For example, you must specify the signals that indicate that the Data Communications Equipment (DCE) is ready to connect. In addition, you might need to adjust the amount of attenuation that the DSL Terminator should apply to the line’s network interface in order to match the cable length from the DSL Terminator to the next repeater.

To configure the nailed T1 line, perform the following tasks:

- Supply information, such as encoding, framing, and buildout (attenuation) that you obtain from your carrier
- Activate the port

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

This section provides background information about the T1 line interface parameters.

Parameter	Description
Framing Mode	The framing used by the physical layer of the T1 line may be D4 or ESF. D4 format, also known as the superframe 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.
Encoding	Sets the Layer 1 line encoding used for the physical links, which affects the way data is represented by the digital signals on the line. Your carrier can tell you which encoding to use. AMI (the default) specifies Alternate Mark Inversion encoding. B8ZS specifies that the encoding is Bipolar with 8-Zero Substitution. The other option, None, is identical to AMI but without density enforcement
Build out	Specifies the amount of attenuation to apply to the T1 transceiver's internal CSU. The amount depends on the cable length from the DSL Terminator to the next repeater. Valid values are 0 db (decibels) through 22.5 db. Attenuation is a measure of the power lost on a transmission line or on a portion of that line. When you specify a value for Buildout, the unit applies attenuation to the T1 line, causing the line to lose power. Repeaters boost the signal on a T1 line. If the unit is too close to a repeater, you might need to add some attenuation. Check with your carrier to determine the correct value.
Clock Source	Indicates whether the T1 line can be used as the master clock source for synchronous connections. In synchronous transmission, both the sending device and the receiving device must maintain synchronization in order to determine where one block of data ends and the next begins. Disable this parameter on one unit if two units connect to each other by a crossover cable (with optional T1 repeaters) between their network ports.
First DS0 Channel Last DS0 Channel	Specifies the number of channels provisioned for your line. Check with your carrier to determine the correct value.

Configuring the nailed T1 line

To configure the nailed T1 line, proceed as in the following example:

1 Open the Net/8T1 Profile.

2 Open the Factory line profile:

```
10-1** Factory
  Line 1...
  Line 2...
  Line 3...
  Line 4...
  Line 5...
  Line 6...
  Line 7...
  Line 8...
```

3 Open a T1 profile:

```
Line 1...
  Enabled=Yes
  Nailed Group=1
  Framing Mode=ESF
  Front End=CSU
  Encoding=B8ZS
  Length=N/A
  Buildout=0dB
  Clock Source=Yes
  First DS0 channel=1
  Last DS0 channel=24
```

4 Enable the line.

```
Enabled=Yes
```

5 Specify a Nailed Group number:

```
Nailed Group=1
```

A Connection profile uses this permanent link by specifying the nailed channels' group number in the Group parameter. A Frame Relay profile uses a permanent nailed link by specifying the group number in its Nailed Group parameter.

6 Set the T1 framing mode.

```
Framing Mode=D4
```

7 Set the Encoding parameter as specified by your carrier.

```
Encoding=B8ZS
```

8 Set the buildout if appropriate.

```
Build Out=0db
```

9 Specify the Clock Source.

```
Clock Source=Yes
```

10 Enter the first and last DS0 channels assigned to this line by your carrier.

```
First DS0 Channel=1
Last DS0 Channel=24
```

11 Save and exit the T1 line profile.

Using T1 line diagnostics

The DSL Terminator provides the following T1 status windows to diagnose the connection:

```
10-000 Net/8T1
   10-100 Line 1 Stat
   10-200 Line Error
```

You can use the preceding settings to gather information about the line. They are located in the Main Status Window status menu. For details about each option, see the *DSL Terminator Reference*.

Configuring E1 lines

DSL Terminator E1 connections are not channelized, but you can configure the E1 line with any number of DS0 channels, up to 32, as specified by your carrier.

With a nailed E1 line, you must manually configure some port information. For example, you must specify the signals that indicate that the DCE is ready to connect. In addition, you might need to indicate the cable length from the Pipeline to the CSU.

To configure the nailed E1 line, you perform the following tasks:

- Specify a group number associated with the nailed E1 line
  You assign a group number to the line and then specify that group number in Connection Profiles that will access the WAN across this interface.
- Supply carrier information, such as encoding, framing, and buildout (attenuation)
- Activate the port

For details on each parameter discussed in the following section, see the *DSL Terminator Reference.*

E1 framing

The framing used by the physical layer of the E1 line may be G.703 (the standard framing mode used by most E1 ISDN providers) and by DASS 2 or 2DS (a variant of G.703 required by most E1 DPNSS providers in the U.K.).

Clock source for synchronous transmission

The clock source determines whether the E1 line can be used as the master clock source for synchronous connections. In synchronous transmission, both the sending device and the receiving device must maintain synchronization in order to determine where one block of data ends and the next begins.

How the DS0s are used

You must specify how the DSOs are used. Ending DS0 Channel specifies the last channel in your line. Enable Channel 16 specifies whether channel 16 is used for data, or whether the unit should ignore it.

Configuring the nailed E1 line

To configure the nailed E1 line, proceed as in the following example:

1. Open the Net/8E1 Profile.
2. Open the Factory line profile:

```
10-1** Factory
  Line 1...
  Line 2...
  Line 3...
  Line 4...
  Line 5...
  Line 6...
  Line 7...
  Line 8...
```

3. Open an E1 profile:

```
  Line 1...
    Enabled=Yes
    Nailed Group=1
    Framing Mode=G.703
    Front End=CSU
    Encoding=B8ZS
    Length=N/A
    Buildout=0dB
    Clock Source=Yes
    First DS0 channel=1
    Last DS0 channel=32
```

4. Enable the line.

   `Enabled=Yes`

5. Specify a Nailed Group number:

   `Nailed Group=1`

   A Connection profile uses this permanent link by specifying the nailed channels' group number in the Group parameter. A Frame Relay profile uses a permanent nailed link by specifying the group number in its Nailed Group parameter.

6. Set the T1 framing mode.

   `Framing Mode=G.703`

7. Set the Encoding parameter as specified by your carrier.

   `Encoding=B8ZS`

8. Set the buildout if appropriate.

   `Build Out=0db`

9. Specify the Clock Source.

   `Clock Source=Yes`

10. Enter the first and last DS0 channels assigned to this line by your carrier.

```
First DS0 Channel=1
Last DS0 Channel=32
```

11. Save and exit the E1 line profile.

Using E1 line diagnostics

The DSL Terminator provides the following E1 status windows to diagnose the connection:

```
10-000 Net/8E1
   10-100 Line 1 Stat
   10-200 Line Error
   10-300 Net Options
```

You can use the preceding settings to gather information about the line. They are located in the Main Status Window status menu. For details about each option, see the *DSL Terminator Reference*.

Configuring Individual WAN Connections 4

Understanding the Answer profile 4-1

Understanding Connection profiles 4-4

Understanding Names/Passwords profiles 4-15

Configuring PPP connections 4-16

Configuring PPP over Ethernet (PPPoE) 4-26

Configuring PPP over ATM 4-30

This chapter describes how to configure various types of links across the WAN. It focuses on the encapsulation issues for Point-to-Point Protocol (PPP) connections. PPP and its multilink variants (MP and MP+) enable connections to use one or more channels. The remote devices must have PPP software.

This chapter does not describe RADIUS user profiles that serve the same function as resident Connection profiles. If you are using a RADIUS authentication server, see the *TAOS RADIUS Guide*. For details about WAN connection security, see Chapter 2, "Setting Up Security."

Understanding the Answer profile

The Answer profile determines whether the DSL Terminator answers or drops an incoming call. If the call does not comply with the specifications in the Answer profile, the DSL Terminator drops the call without answering it.

Most administrators set up the Answer profile to reject calls that do not match a Connection profile. When a call matches a Connection profile, the DSL Terminator uses the connection-specific settings instead of the encapsulation and session settings in the Answer profile. However, if you configure a Names/Passwords profile, the DSL Terminator can use the settings in the Answer profile to build the session. Following are the Answer profile parameters:

```
Ethernet
   Answer
      Use Answer as Default=No
      Force 56=No
      Profile Reqd=Yes
      Assign Adrs=No

      Encaps...
         MPP=Yes
```

```
   MP=Yes
   PPP=Yes
   FR=Yes


IP options...
   Metric=7

PPP options...
   Route IP=Yes
   Bridge=Yes
   Recv Auth=None
   MRU=1524
   LQM=No
   LQM Min=600
   LQM Max=600
   Link Comp=Stac
   VJ Comp=Yes
   BACP=No
   Dyn Alg=Quadratic
   Sec History=15
   Add Pers=5
   Sub Pers=10
   Min Ch Count=1
   Max Ch Count=1
   Target Util=70
   Idle Pct=0
   Disc on Auth Timeout=Yes

Session options...
   RIP=Off
   Data Filter=5
   Call Filter=3
   Filter Persistence=No
   Idle=120
   Max Call Duration=0
   Preempt=N/A

DHCP options...
   Reply Enabled=No
   Pool Number=N/A
   Max Leases=N/A
```

The table below provides some information about the parameters in the Answer profile. For detailed information about each parameter, see the *DSL Terminator Reference Guide*.

Parameter	Description
Use Answer as Default	Specifies whether the Answer profile should override the factory defaults when the DSL Terminator uses RADIUS or TACACS to validate an incoming call.
Force56	Specifies whether the DSL Terminator uses only the 56Kbps portion of a channel, even when all 64Kbps appear to be available. To force the DSL Terminator to use only 56Kbps, set this parameter to Yes. The default setting is No.

Profile Reqd	Specifies if the DSL Terminator requires a Connection profile for every caller. With the No setting, the DSL Terminator builds a temporary profile for an unknown caller. Many sites consider a Profile Reqd parameter setting of No, a security breach. **Note:** Setting the Profile Reqd parameter to Yes disables Guest access for ARA connections.
Assign Adrs	Enables or disables dynamic IP address assignment for incoming calls. The default setting is no.
Encaps subprofile	Contains settings for each type of link encapsulation that the DSL Terminator supports. With a No setting in this submenu, the unit does not accept calls of that type. For the details about PPP and other encapsulation options, see "Encapsulation options" on page 4-6. The Answer profile uses these options only when you have not set the corresponding options in the caller's configured Connection profile.
PPP options	Contains settings for PPP routing parameters needed for initial negotiation for incoming callers.
IP options	Contains setting for IP routing parameters needed for initial negotiation for incoming callers.
Session options	Contains settings for default filters and timers for building connections that use RADIUS (if you enable Use Answer as Defaults) or Names/Passwords profiles.
DHCP options	Enables the DSL Terminator to act as a DHCP server for a local Pipeline unit for connections that use RADIUS (if you enable Use Answer as Defaults) or Names/Passwords profiles.

Example of Answer profile configuration

When a call first comes in, it is unauthenticated. The Answer profile lets you negotiate the PPP, authentication, encapsulation methods, and lets you set whether the call will route or bridge. After the connection authenticates, the DSL Terminator uses the appropriate Connection profile or, if RADIUS is configured, the DSL Terminator uses the appropriate User profile.

To set up the profile:

1. Open the Answer profile and set Profile Reqd to Yes.
2. Enable dynamic assignment of IP addresses to callers, if appropriate.

```
Ethernet
  Answer
   Profile Reqd=Yes
   Assign Adrs=No
```

3. Make sure you enable the encapsulation types you intend to support. For example:

```
Encaps...
 MPP=Yes
 MP=Yes
 PPP=Yes
 FR=Yes
```

4 Enable routing and bridging and specify authentication requirements, as appropriate. For example:

```
PPP options...
 Route IP=Yes
 Bridge=Yes
 Recv Auth=Either
```

5 Close the Answer profile.

Understanding Connection profiles

A Connection profile defines individual connections. For a given encapsulation type, the Connection profile contains many of the same options as the Answer profile.

Note: Settings in a Connection profile always override similar settings in the Answer profile.

Following are the Connection profile parameters (shown with sample settings):

```
Ethernet
   Connections
     any Connection profile
       Station=device-name
       Active=Yes
       Encaps=FR
       PRI # Type=N/A
       NumPlanID=ISDN
       Dial #=N/A
       Route IP=Yes
       Bridge=No
       Dial brdcast=N/A
       Shared Prof=No

       Encaps=encapsulation-protocol
       Encaps options...
         parameters for selected encapsulation-protocol
       IP options...
         LAN Adrs=0.0.0.0/0
         WAN Alias=0.0.0.0/0
         IF Adrs=0.0.0.0/0
         Preference=60
         Metric=7
         DownPreference=100
         DownMetric=1
         Private=No
         SourceIP Check=No
         RIP=Off
         Pool=0
         Multicast Client=No
         Multicast Rate Limit=5
         Multicast Grp Leave Delay=0
         Client Pri DNS=0.0.0.0
         Client Sec DNS=0.0.0.0
         Client Assign DNS=Yes
         Client Gateway=0.0.0.0
         TOS Enabled=No
         Precedence=N/A
```

```
   TOS=N/A
   Apply to=N/A
   TOS Filter=0

Session options...
   Data Filter=5
   Call Filter=3
   Filter Persistence=No
   Idle=N/A
   Max Call Duration=0
   Preempt=N/A
   BackUp=connection profile name
   Block calls after=0
   Blocked duration=0
   Ses Rate Type=disabled
   Ses Rate Mode=N/A
   Ses Line Rate= N/A
   Rx Data Rate Limit=0
   Tx Data Rate Limit=0
   IP Direct=0.0.0.0
   ATMP Gateway=N/A
   Max ATMP Tunnels=N/A
   ATMP RIP=N/A
   FR Direct=No
   FR Prof=N/A
   FR DLCI=N/A


Telco options...
   AnsOrig=Both
   Callback=No
   Exp Callback=No
   Callback Delay=N/A
   Call Type=Switched
   Group=N/A
   FT1 Caller=N/A
   Data Svc=56KR
   Force 56=N/A
   Bill #=555-1212
   Call-by-Call=N/A
   Transit #=222
   NAS Port Type=Any

Accounting...
   Acct Type=None
   Acct Host=N/A
   Acct Port=N/A
   Acct Timeout=N/A
   Acct Key=N/A
   Acct-ID Base=N/A

DHCP options...
   Reply Enabled=No
   Pool Number=N/A
   Max Leases=N/A
```

Note: After you select an encapsulation method in the Encaps option, the Encaps Options subprofile contains settings related to the selected type.

For information on IP, and bridging configuration, see the appropriate chapter in this guide. For detailed information about each parameter, see the *DSL Terminator Reference.*

Connection profile parameters

This section provides some background information about Connection profile parameters.

Parameter	Description
Station	Name of the remote device. Make sure that the Station name matches the remote device's name exactly, including case changes.
Active	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.
Encaps	Specify an encapsulation protocol for each connection. Set additional options for the configured protocol in the Encaps Options subprofile, described in "Encaps Options subprofile parameters" on page 4-8.
PRI # Type	Specifies the TypeOfNumber field in the called party's information element. PRI # Type 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 the proper setting to use.
NumPlanID	Specifies NumberPlanID field in the called party's information element. 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 the proper setting to use.
Dial #	Specifies the number used to dial out this connection. This value can contain up to 24 characters, which can include a dialing prefix that directs the connection to use a trunk group or dial plan, for example, 6-1-212-555-1212.
Route IP	Each connection can be configured for IP routing. Each of these routing setups has a separate subprofile within a Connection profile.
Bridge	Link-level bridging forwards packets to and from remote networks on the basis of the hardware-level address, not a logical network address.
Dial brdcast	Specifies whether the DSL Terminator will dial this connection when it receives Ethernet broadcast packets. By default, the DSL Terminator does not dial on broadcast; it relies on its internal bridging table to bring up specific bridged connections.
Shared Prof	Enables the DSL Terminator to force terminal server users to connect using unique profiles.

Encapsulation options

You can set the Encaps parameter to MP+, MP, FR, FR_CIR, PPP, ATM, or ATM-FR_CIR. The Encaps Options subprofile parameters vary depending on the type of encapsulation you have set under the Encaps parameter.

MP+ or MP encapsulation

When the Connections > *Connection profile* > Encaps parameter is set to MP+ or MP, the following parameters appear in the interface for Ethernet > Connections > *Connection profile*> Encaps Options. The Encaps Options subprofile defines authentication-protocol values between the DSL Terminator and the far end device.

```
Ethernet
  Connections
   Connection profile
    Encaps options...
      Send Auth
      Send Auth=None
      Bi-dir Auth=N/A
      Send PW=
      Aux Send PW=N/A
      Recv Name=N/A
      Recv PW=
      DBA Monitor=Transmit
      Base Ch Count=1
      Min Ch Count=1
      Max Ch Count=2
      Inc Ch Count=1
      Dec Ch Count=1
      MRU=1524
      LQM=No
      LQM Min=600
      LQM Max=600
      Link Comp=None
      VJ Comp=No
      Dyn Alg=Quadratic
      Sec History=15
      Add Pers=5
      Sub Pers=10
      Target Util=70
      Idle Pct=0
      Split Code.User=N/A
```

PPP Encapsulation

When the Connections > *Connection profile* > Encaps parameter is set to PPP, the following parameters appear in the interface for Ethernet > Connections > *Connection profile*> Encaps Options and define authentication-protocol values between the DSL Terminator and the far end device

```
Ethernet
  Connections
   Connection profile
    Encaps options...
      Send Auth
      Bi-dir Auth=N/A
      Send PW=
      Recv Name=N/A
```

```
      Recv PW=
      MRU=1524
      LQM=No
      LQM Min=600
      LQM Max=600
      Link Comp=None
      VJ Comp=No
      Split Code.User=N/A
```

ATM or ATM-FRF_CIR encapsulation

When the Connections > *Connection profile* > Encaps parameter is set to ATM or ATM-FRF_CIR, the following parameters appear in the interface for Ethernet > Connections > *Connection profile*> Encaps Options. The Encaps Options subprofile defines authentication-protocol values between the DSL Terminator and the far end device

```
Ethernet
  Connections
    Connection profile
     Encaps options...
       vpi=8
       vci=35
       Circuit=N/A
       Inverse Arp=No
       FRF.8 Mode=N/A
```

FR or FRF_CIR encapsulation

When the Connections > *Connection profile* > Encaps parameter is set to FR or FRF_CIR, the following parameters appear in the interface for Ethernet > Connections > *Connection profile*> Encaps Options. The encaps options subprofile defines authentication-protocol values between the DSL Terminator and the far end device.

```
Ethernet
  Connections
    Connection profile
      Encaps options...
       FR Prof=
       DLCI=16
       Circuit=N/A
       MFR Bundle Name=
```

Encaps Options subprofile parameters

Following is an overview of the Encaps Options subprofile parameters

Parameter	**Specifies**
Send Auth	Authentication protocol that the DSL Terminator uses to send a password to the far end of a PPP connection.

Parameter	Specifies
Send Name	Name that the DSL Terminator sends to the far end device during PPP authentication. Authentication fails if the name does not match what the far end device expects or if either the password or IP address (for IP-routed connections) for the Connection profile does not match what the far end device expects. Specify up to 16 characters. The default is null.
Send PW	Password that the DSL Terminator sends to the far end while the connection is being authenticated. If this password is not received by the far end device, authentication fails.
Aux Send PW	Password that the DSL Terminator sends when it adds channels to a multichannel PPP call that uses PAP-TOKEN-CHAP authentication. The DSL Terminator obtains authentication of the first channel of this call from the user's hand-held security card.
Recv PW	Password that the DSL Terminator 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. For PPP links, the password can contain up to 20 characters.

DBA monitoring and channel allocation parameters

The following parameters in Ethernet > Connections > *Connection profile* > Encaps Options subprofile and define the monitoring of Dynamic Bandwidth Allocation (DBA) and the number of used with MP+ calls:

Parameter	Specifies
DBA Monitor	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, DBA is disabled.
Base Ch Count	Number of channels to use to set up a session initially. If the session uses MP, Base Ch Count specifies the total number of channels to be used for the call. For an AIM, BONDING, or multichannel PPP call, the channel count may be augmented.
Min Ch Count	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, set this parameter to the same value on both sides of the multilink connection.
Max Ch Count	Maximum number of channels that can be allocated to a multilink connection. For optimum performance, set this parameter to the same value on both sides of the multilink connection.
Inc Ch Count	Number of channels that the DSL Terminator adds when bandwidth changes either manually or automatically during a call.
Dec Ch Count	Number of channels that the DSL Terminator removes when bandwidth changes either manually or automatically during a call. You cannot clear a call by decrementing channels.

MRU, LQM, and Compression parameters

The following parameters in Ethernet > Connections > *Connection profile* > Encaps Options subprofile define the number of bytes the DSL Terminator can receive in a single frame, Link Quality Monitoring (LQM) values and link compression settings for packets and for headers.

Parameter	Specifies
MRU	Maximum number of bytes the DSL Terminator can receive in a single frame. Usually the default is the correct setting, unless the far end requires a lower number.
LQM	Whether or not the DSL Terminator requests 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.
LQM Min	Minimum duration between link-quality reports for PPP connections, measured in 10ths of a second.
LQM Max	Maximum duration between link-quality reports for PPP connections, measured in 10ths of a second.
Link Comp	Link-compression method for a PPP, MP, and MP+ calls. Set the same type of link compression on both sides of the connection, otherwise link compression is not used.
VJ Comp	Whether or not Van Jacobsen IP header compression should be 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.

FR and FR_CIR

When Connections > *Connection profile* > Encaps parameter is set to FR or FR_CIR, the following parameters appear in the interface for Ethernet > Connections > *Connection profile* > Encaps Options subprofile:

Parameter	Specifies
FR Prof	Name of the Frame Relay profile to use for forwarding this link on the Frame Relay network.
DLCI	Frame Relay DLCI number for a gateway or circuit connection. A Data Link Connection Indicator (DLCI) is a number between 16 and 991, that 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.
Circuit	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.

ATM and ATM-FRF_CIR

When the Connections > *Connection profile* > Encaps parameter is set to ATM or ATM-FRF_CIR, the following parameters appear in the interface for Ethernet > Connections > *Connection profile*> Encaps Options subprofile and define authentication protocol values between the DSL Terminator and the far end device.

Parameter	**Specifies**
VPI	Virtual Path Identifier (VPI) for the connection. Specify a number from 0 to 15. The default is 0 (zero).
VCI	The Virtual Circuit Identifier (VCI) for the connection. Specify a number from 32 to 1023. The default is 32.
Circuit	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.
FRF.8 Mode	Mode of operation for the ATM-Frame Relay circuit. Translation mode causes the system to convert RFC 1490 encapsulation to RFC 1483 for Frame to ATM traffic. Encapsulation is converted from 1483 to 1490 for ATM to Frame traffic. Translation mode is the default. Transparent mode data passes from one circuit to the other without translation.

Connection profile: Ip Options subprofile parameters

This section provides some background information about the for Ip Options subprofile parameters.

LAN Adrs	Specifies the IP address of remote-end host or router.
WAN Alias	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 Adrs	Specifies a numbered interface IP address for the DSL Terminator. Interface-based routing allows the DSL Terminator to operate more nearly the way a multi-homed Internet host behaves.
Preference	Specifies the preference value for a route.
Metric	Specifies a RIP metric (a virtual hop count) associated with the IP route.
DownPreference	Specifies the preference value for a route whose associated WAN connection is down.
DownMetric	Specifies the metric for a route whose associated WAN connection is down.
Private	Specifies whether the DSL Terminator discloses the existence of this route when queried by RIP or another routing protocol. Private routes are used internally but are not advertised
RIP	Specifies how the DSL Terminator handles RIP update packets on the interface.

Pool	Specifies an IP address pool from which the caller will be assigned an IP address. If the Pool parameter is null but all other configuration settings enable dynamic assignment, the DSL Terminator gets IP addresses from the first defined address pool.
Client Pri DNS	Specifies a primary DNS server address to be sent to any client connecting to the DSL Terminator. 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.
Client Sec DNS	Specifies a secondary DNS server address to be sent to any client connecting to the DSL Terminator. 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.
Client Assign DNS	Specifies whether client DNS server addresses are presented while this connection is being negotiated.
Client Gateway	Specifies a connection-specific default route to be used for forwarding packets received on this connection. The DSL Terminator uses this default route instead of the system-wide Default route in its routing table. This route is connection-specific, so it is not added to the routing table.

Connection profile: Session options subprofile

This section provides a brief overview of the Connection profile Session Options subprofile parameters. For detailed information about each parameter, see the *DSL Terminator Reference Guide*.

Parameter	**Description**
Data Filter, Call Filter	Lucent filters that define packet conditions. Data filters drop specific packets, and are often used for security purposes. Call filters monitor inactive sessions and bring them down to avoid unnecessary connection costs. When a filter is in use, the DSL Terminator examines every packet in the packet stream and takes action if the defined filter conditions are present. The action that the DSL Terminator takes depends both on the conditions specified within the filter and how the filter is applied. (For more information, see Chapter 11, “Defining Static Filters.”)
Idle	Specifies how long the connection remains idle before the DSL Terminator drops it.

Max Call Duration	Sets the maximum duration of an incoming call. Enter a value from 1 up to 1440 minutes. The default, 0 (zero), turns off this function. The DSL Terminator checks the connection once a minute, so the actual time of the call can be slightly longer than the number of minutes you set.
Preempt	Specifies the number of idle seconds the DSL Terminator waits before it can use one of the channels of an idle link for a new call.
Backup	Specifies the name of a Connection profile to use when a nailed connection goes down. For example, if a nailed connection to corporate net #1 is out of service, you can use a backup switched connection to corporate net #2. You cannot use this parameter to provide alternative lines to a single destination.

Connection profile: Telco Options subprofile

This section provides a brief overview of the Connection profile Telco Options subprofile parameters. For detailed information about each parameter, see the *DSL Terminator Reference Guide*.:

Parameter	**Specifies**
AnsOrig	Whether or not the DSL Terminator will enable incoming calls, outgoing calls, or both, for this connection.
Callback	Whether or not the callback feature is enabled. If enabled, the DSL Terminator hangs up after receiving an incoming call that matches the one specified in the Connection profile. The DSL Terminator then calls back the device at the remote end of the link using the Dial # specified in the Connection profile.
Exp Callback	Whether or not 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.
Callback Delay	Elapsed time before DSL Terminator calls back the device at the remote end.
Call Type	Type of connection, or in the case of codecs, the architecture of the connection.
Group	Assigns a group of nailed channels to a connection. For connections whose call type is Nailed/MPP, you can concatenate group numbers by separating them with a comma; for example, Group=1,3,5,7 assigns four groups of nailed channels.
FT1 Caller	Whether or not the DSL Terminator initiates an FT1-AIM, FT1-B&O, or Nailed/MPP call, or whether it waits for the remote end to initiate these types of calls. If the remote end has FT1 Caller set to No, set it to Yes on the local DSL Terminator; by the same token, if the remote end has FT1 Caller set to Yes, set it to No on the local DSL Terminator.

Parameter	Specifies
Data Svc	Type of data service that the link uses. 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.
Bill #	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.
Call-by-Call	PRI service to use when placing a call using that profile. The Call-by-Call setting in the Dial Plan profile overrides the Call-by-Call setting in the Call and Connection profiles.
Transit #	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.
NAS Port Type	Type of calls that can be received.

The `Call Type=Switched` setting is the default. The other options are for nailed, nailed-MP+, and permanent switched connections.

A nailed connection is a permanent link that is always up as long as the physical connection persists. For a nailed connection, you must specify the group number of the nailed channels. You can even combine groups of nailed channels to create a single high-speed nailed connection. For example:

```
Call Type=Nailed
Group=3, 4
```

A nailed/MP+ connection combines nailed and switched channels. When you choose this Call Type, you need to set the FT1 Caller parameter to specify which side of the link can add switched channels.

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 terminates, the permanent switched connection attempts to restore the link at 10-second intervals, similar to the way in which the DSL Terminator maintains a nailed connection. A permanent switch connection conserves connection attempts but results in a long connection time. The combination can be cost effective for some customers. For details, see the *DSL Terminator Reference Guide*.

Connection profile: Accounting subprofile parameters

This section provides a brief overview of the Connection profile Accounting subprofile parameters. For detailed information about each parameter, see the *DSL Terminator Reference Guide*.

Parameter	Specifies
Acct Type	Whether this connection uses the default accounting setup (specified in the Ethernet profile), no accounting at all, or the user-specific setup specified here. The DSL Terminator supports both RADIUS and TACACS+ accounting.
Acct Host	IP address of a Connections-specific accounting server to use for information related to this link.
Acct Port	UDP port number that the Lucent unit uses in accounting requests.
Acct Timeout	Sets the amount of time the DSL Terminator waits for a response to a RADIUS accounting request. You can set this parameter globally and for each Connection. TACACS+ has its own timeout method.
Acct Key	RADIUS or TACACS+ shared secret. A shared secret acts like a password between the DSL Terminator and the accounting server.
Acct-ID Base	Whether or not the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16. It controls how the Acct-Session-ID attribute is presented to the accounting server; for example, a base-10 session ID is presented as 1234567890, and a base-16 ID as 499602D2. You can set this parameter globally and for each Connections.

Understanding Names/Passwords profiles

Names/Passwords profiles provide simple name and password authentication for incoming connections. They are used only if authentication is required in the Answer profile (Recv Auth).

Names/Passwords profiles include the following parameters (shown with sample settings):

```
Ethernet
   Names / Passwords
      Name=Brian
      Active=Yes
      Recv PW=brianpw
      Template Connection #=0
```

Names and Passwords profile parameters

This section provides some background information about Names and Passwords profiles. (For detailed information, see the *DSL Terminator DSL Terminator Reference*.

Parameter	Description
Name	Name specified by the incoming connection request, including case changes. Lucent does not recommend that you specify a name that is already in use in a Connection profile. The name can be up to 31 characters.
Active	Enables a Names/Passwords profile for use. Set the Active parameter to Yes to enable the profile. If you are using a Template connection profile to build the session, that profile must also be active. (The Template Connection parameter specifies the template profile.)
Rec PW	Specify a password that exactly matches the incoming connection requestor, including case changes. The password can be up to 20 characters.
Template Connection	To use a Template Connection profile rather than the Answer profile settings to build the session for this Names/Passwords profile, specify the unique portion of the profile's number here. The default, 0 (zero), instructs the DSL Terminator to use the Answer profile settings. Any other number denotes a Connection profile. The specified Connection profile must be active. Template connections can be used to enable or disable group logins.

Example Names/Passwords profile configuration

To configure a Names/Passwords profile that uses the Answer profile settings:

1. Open a Names/Passwords profile.
2. Specify the user's name and password, and activate the profile. For example:

```
Ethernet
   Names / Passwords
      Name=Brian
      Active=Yes
      Recv PW=brianpw
      Template Connection #=0
```

3. Leave the Template Connection # set to **0** (zero) to use Answer profile settings.
4. Close the profile.

Configuring PPP connections

A PPP connection can be one of the following types:

- PPP—A single-channel connection to any remote device running PPP software.
- Multilink PPP (MP)—A multilink connection to an MP-compliant device from any vendor.

- MP with Bandwidth Allocation Control Protocol (MP with BACP)—An MP call that uses BACP to increase or decrease bandwidth on demand.
- Multilink Protocol Plus (MP+)—A multilink connection, to another MAX unit, that uses dynamic bandwidth allocation to increase or decrease bandwidth on demand.

Note: MP+ supersedes MP.

A multilink connection begins by authenticating a base channel. If the connection allows additional bandwidth, the local or remote unit dials another link. For example, if a dial-in Lucent Pipeline unit has a single-channel session at 56 Kbps or 64 Kbps and multilink PPP is configured, a second call can combine the first B channel with the second for a transmission rate of 112 Kbps or 128 Kbps.

DSL Terminator units can be *stacked* to distribute the bandwidth required for connections across multiple units (as described in).

Note: If a connections configured for multilink PPP fails to establish multiple channels, it falls back to a single-channel PPP session. In either case, you can use the PPP parameters as part of the connection negotiation. Use the MP, BACP, and MP+ settings *in addition to* the single-channel PPP settings.

To establish a single-channel PPP call or the base channel of a multilink PPP call, set the necessary parameters for PPP negotiation as in the following example (shown with sample settings):

```
Ethernet
  Answer
    Encaps
      PPP=Yes
    PPP Options
      Route IP=Yes
      Bridge=Yes
      Recv Auth=Either
      MRU=1524
      LQM=No
      LQM Min=600
```

Understanding the PPP Options subprofile parameters

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

Note: You must enable routing or bridging in the Answer profile for the DSL Terminator to pass the data stream from an answered call to its internal bridge/router software.

Parameter	Description
Revc Auth	Specifies the protocol to use for authenticating the password sent by the far end during PPP negotiation. You can specify None, PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MS-CHAP (Microsoft Challenge Handshake Authentication Protocol format supported by Windows NT systems), or Either. The Either setting allows any of the above. The far end device must also support the specified protocol.
Send Auth	In the Connection profile's Encaps Options subprofile, the Send Auth parameter specifies that protocol to use for the password sent to the far end during PPP negotiation.
Send PW	In the Connection's profile's Encaps Options subprofile, the Send PW parameter is the password sent to the remote device. It must match the password expected from the DSL Terminator.
Recv PW	The password sent to the DSL Terminator from the remote device. It is used to match up the caller to a profile when IP routing is not in use.
Send Name	Specifies the name that the DSL Terminator sends to the far end device during PPP authentication. Authentication fails if the name does not match what the far end device expects. Also, authentication fails if either the password or IP address (for IP-routed connections) for the Connection profile does not match what the far end device expects. Specify a string of up to 16 characters. The default value is null.
Maximum receive units (MRU)	In the Answer's profiles's PPP Options, the MRU parameter specifies the maximum number of bytes the DSL Terminator can receive in a single packet on a PPP link. Leave this parameter at the default value of 1524, unless the far end device requires a lower number.
MTU-Limit	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.
Link quality monitoring (LQM)	Specify whether the DSL Terminator monitors the quality of the link. If the LQM parameter is set to Yes, you can specify the minimum and maximum duration between reports, measured in tenths of a second. 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. For a connection that has a Connection profile, that profile's LQM settings take precedence over the LQM settings in the Answer profile.

Link Comp	Specifies the type of link compression for the connection. By default the default setting is None. For additional information, see “Link Comp and VJ Comp” on page 4-19.
VJ Comp	VJ Comp specifies the type of TCP/IP header compression. By default the default setting is No. For additional information, see “Link Comp and VJ Comp” on page 4-19.
BACP	Enables the Bandwidth Allocation Control Protocol. The DSL Terminator encapsulates connections in MP (RFC 1990) and uses BACP to manage dynamic bandwidth on demand. Both sides of the connection must support BACP. BACP uses the same criteria for managing bandwidth dynamically as MP+ connections. Specify either Yes to enable BACP or No to disable BACP. No is the default.
Dyn Alg	Specifies the algorithm that the DSL Terminator uses to calculate average line utilization (ALU). Select one of the following values: • Quadratic—the DSL Terminator gives preference to recent samples of bandwidth usage than to older samples taken in the number of seconds specified in Sec History. The preference grows at a quadratic rate. The default is Quadratic. • Linear—The DSL Terminator gives preference to recent samples of bandwidth usage than to older samples taken in the number of seconds specified in Sec History. The weighting grows at a linear rate. • Constant—The DSL Terminator does not give greater preference to recent samples.
Sec History	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.
Split Code.User	Divides the PIN and CODE of a user and their USERNAME by a period. Enable this feature if the CHAP field cannot accommodate the full PIN+CODE.USER value. The DSL Terminator splits the passcode into two pieces with the information following the period becoming the CHAP Name, overriding the name of the router. Specify Yes to enable the PIN, CODE and USERNAME to be divided. Specify No to disable the feature. No is the default.

Link Comp and VJ Comp

In the Answer profile and in Connection profiles, the Link Comp parameter specifies the type of link compression for the connection, and VJ Comp specifies the type of TCP/IP header compression. By default, the Link Comp parameter is set to None and the VJ Comp parameter is set to No.

For data compression to take effect, both sides of a connection must support it. The DSL Terminator supports Stac and MS-Stac compression for PPP-encapsulated calls.

Stac compression is the Stacker LZS compression algorithm, developed by STAC Electronics, Inc., that modifies the standard LZS compression algorithm to optimize for speed (as opposed

to optimizing for compression). Stac compression is one of the parameters negotiated when setting up a PPP connection.

MS-Stac refers to Microsoft LZS Coherency compression for Windows 95. This is a proprietary compression scheme for Windows 95 only (not for Windows NT).

Note: If the caller requests MS-Stac and the matching profile does not specify MS-Stac compression, the connection seems to come up correctly but no data is routed. If the profile is configured with MS-Stac and the caller does not acknowledge that compression scheme, the DSL Terminator attempts to use standard Stac compression, and if that does not work, it uses no compression.

Novell's NetWare relies on the Data Link layer (also called Layer 2) to validate and guarantee data integrity. STAC link compression, if specified, generates an eight-bit checksum, which is inadequate for NetWare data.

If your DSL Terminator supports NetWare (either routed or bridged) and you require link compression, disable link compression as follows:

- Set Ethernet > Answer > PPP Options > Link Comp = None.
- Set Ethernet > Connections > *Any Connection profile* > Encaps Options > Link Comp = None.

By disabling link compression, the DSL Terminator validates and guarantees data integrity by means of PPP.

VJ Comp applies only to packets in TCP applications, such as Telnet. When you turn it on, the DSL Terminator applies TCP/IP header compression for both ends of the link.

Example of a PPP connection

To configure a basic PPP connection, proceed as follows:

1 Make sure the Answer profile enables PPP encapsulation and has the appropriate routing, bridging, and authentication settings. For example:

```
Ethernet
   Answer
      Encaps...
         PPP=Yes

      PPP options...
         Route IP=Yes
         Bridge=Yes
         Recv Auth=Either
```

2 Close the Answer profile.

3 Open a Connection profile.

4 Specify the name of the remote device and activate the profile. For example:

```
Ethernet
  Connections
    Station=tommy
   Active=Yes
```

Note: Make sure that you specify the Station name exactly, including case changes.

5 Select PPP encapsulation and set the appropriate PPP options. For example:

```
Encaps=PPP
Encaps options...
  Send Auth=CHAP
  Send PW=remotepw/A
  Recv PW=localpw
```

The Send Auth parameter should be set to CHAP or PAP. Both sides of the connection must support the selected authentication protocol and the selected compression methods.

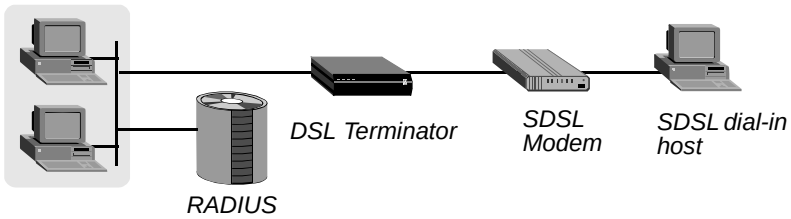
6 Close the Connection profile.

Setting up a PPP connection using RADIUS

Point-to-Point Protocol (PPP) enables you to set up a single-channel connection to any other device running PPP. A PPP connection can support IP routing, protocol-independent bridging, and password authentication using PAP, CHAP, or MS-CHAP.

A PPP connection is usually a bridged or routed network connection initiated in PPP dialup software. Figure 4-1 shows the DSL Terminator unit with a PPP connection to a remote user running Windows 95 with PPP dialup software.

Figure 4-1. A PPP connection



Before you begin

Before configuring the RADIUS user profile for a PPP connection, you must perform the following tasks:

1 Work with the caller to find out what software and modem device exists at the remote end.

2 Determine the appropriate routing, authentication, and compression settings.

3 For the DSL Terminator unit to use the Answer profile as the default when answering a call, set the Default parameter to Yes in the Ethernet > Answer menu.

If you accept the default setting of No, the DSL Terminator unit uses the factory defaults.

4 In Ethernet > Answer > PPP Options, set the Recv Auth parameter to PAP, CHAP, MS-CHAP, or Either.

If the incoming PPP call does not include a source IP address, the DSL Terminator unit requires PAP, CHAP, or MS-CHAP authentication.

5 To enable PPP encapsulation, set the PPP parameter to Yes in the Ethernet > Answer > Encaps menu.

6 Assign a name to the DSL Terminator unit in the System profile.

Configuring a PPP connection in RADIUS

To configure a PPP connection in RADIUS, use the attributes listed in Table 4-1.

Table 4-1. PPP attributes

Attribute	Description	Possible values
Ascend-Link-Compression (233)	Turns data compression on or off for a PPP link.	Link-Comp-None (0) Link-Comp-Stac(1) The default value is Link-Comp-None.
Ascend-PPP-Address (253)	Specifies the IP address of the DSL Terminator unit as reported to the calling unit during PPP IPCP negotiations.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0, which specifies that IPCP negotiates using the value of the IP Adrs parameter.
Ascend-PPP-Async-Map (212)	Gives the PPP code the async control character map for the PPP session.	Four-byte bitmap to control characters. The default is the standard async control character.
Framed-MTU (12)	Specifies the maximum number of bytes the DSL Terminator unit can receive in a single packet on a PPP link.	Integer between 1 and 1524. The default value is 1524.
Framed-Protocol (7)	Specifies the type of protocol the link can use.	PPP (1) MPP (256) FR (261) FR-CIR (263) ATM-1483 ATM-FR-CIR By default, the DSL Terminator unit does not restrict the type of protocol a link can use.
Password (2)	Specifies the user's password.	Alphanumeric string of up to 252 characters. The default is null.
User-Name (1)	Specifies the user's name.	Alphanumeric string of up to 252 characters. The default is null.
User-Service (6)	Indicates whether the type of framed services the link can use.	Framed-User (2) Dialout-Framed-User (5) By default, the DSL Terminator unit does not restrict the framed services that a link can use.

To configure a PPP connection in a RADIUS user profile, follow these steps:

1. On the first line of the profile, specify the User-Name and Password attributes, and set the User-Service parameter to Framed-User.
2. Set the Framed-Protocol parameter to PPP.
3. To specify the DSL Terminator unit's IP address, set the Ascend-PPP-Address attribute.

   If you do not specify a value for this attribute, or if you specify the value 0.0.0.0, IPCP negotiates using the value of the IP Adrs parameter in the Ethernet > Mod Config > Ether Options menu. If you specify a valid IP address, IPCP negotiates with that IP address. If you set the value of this attribute to 255.255.255.255, IPCP negotiates with the address 0.0.0.0. Note that you can assign Ascend-PPP-Address a value different from the DSL Terminator unit's true IP address, as long as the user requesting access understands that limitation.
4. To specify the async control character map for the PPP session, set the Ascend-PPP-Async-Map attribute.

   The value you specify is a four-byte bitmap to one or more control characters. The async control character map is defined in RFC 1548 and specifies that each bit position represents its ASCII equivalent. The bits are ordered with the lowest bit of the lowest byte being 0 (zero). For example, bit 19 corresponds to Control-S (DC3) or ASCII 19. The control characters pass through the PPP link as data. Only applications running over the link can use these characters.
5. To specify the maximum number of bytes the DSL Terminator unit can receive in a single packet on a PPP link, set the Framed-MTU attribute.

   The default value is 1524. You should accept this default unless the device at the remote end of the link cannot support it. If the administrator of the remote network specifies that you must change this value, specify a number between 1 and 1524.
6. To turn data compression on or off for a PPP link, set the Ascend-Link-Compression attribute.

   – Link-Comp-None (0) turns off data compression. This value is the default.

   – Link-Comp-Stac (1) turns on data compression. The DSL Terminator unit applies the STACKER LZS compression/decompression algorithm.

   Both sides of the link must set either the Ascend-Link-Compression attribute (in RADIUS) or the Link Comp parameter (on the DSL Terminator unit) to turn on data compression.
7. Specify routing or bridging attributes for the connection.

   For details on specifying protocol-independent bridging, see Chapter 8, "Configuring Packet Bridging.".
8. Configure the bridging or routing setup in the DSL Terminator unit for the WAN connection.

   For details, see Chapter 8, "Configuring Packet Bridging." in this guide.

PPP connection example

The following is a sample user profile showing a PPP link that requests link compression and IP routing:

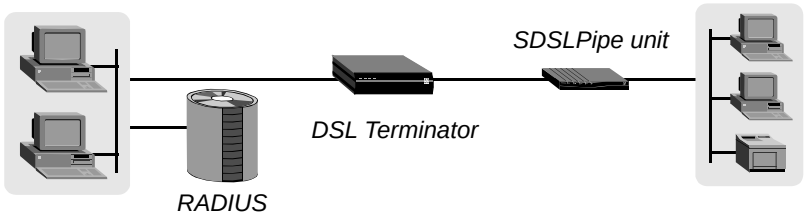
```
Emma Password="m2dan", User-Service=Framed-User
    Framed-Protocol=PPP,
```

```
Framed-Address=200.250.55.9,
Framed-Netmask=255.255.255.248,
Ascend-Link-Compression=Link-Comp-Stac,
Ascend-Route-IP=Route-IP-Yes,
Ascend-Metric=2
```

Setting up an MP or MP+ connection using RADIUS

Both Multilink Protocol (MP) and Multilink Protocol Plus (MP+) connections use PPP encapsulation over a multichannel link. Figure 4-2 shows the DSL Terminator unit connected to a remote SDSLPipe unit with an MP+ connection.

Figure 4-2. An MP+ connection



Other types of units may support MP but not MP+, so if you configure an MP+ connection in RADIUS between the DSL Terminator unit and another type of unit, the DSL Terminator unit first requests the MP+ protocol. If the remote end refuses MP+, the DSL Terminator unit uses MP instead. If the answering device refuses both MP+ and MP, the DSL Terminator unit sets up a PPP call on a single channel.

Before you begin

Before configuring the RADIUS user profile for an MP or MP+ connection, you must perform the following tasks:

1. Work with the caller to find out about the dial-up software and the Lucent configuration at the remote end.
2. Determine the appropriate routing, bridging, and authentication settings for the caller.
3. For the DSL Terminator unit to use the Answer profile as the default when answering a call, set the Default parameter to Yes in the Ethernet > Answer menu.

   If you accept the default setting of No, the DSL Terminator unit uses the factory defaults.
4. In the Ethernet > Answer > PPP Options menu, set the Recv Auth parameter to PAP, CHAP, MS-CHAP, or Either. If the incoming PPP call does not include a source IP address, the DSL Terminator unit requires PAP, CHAP, or MS-CHAP authentication.
5. To enable MP encapsulation, set the MP parameter to Yes in the Ethernet > Answer > Encaps menu.
6. To enable MP+ encapsulation, set the MPP parameter to Yes in the Ethernet > Answer > Encaps menu.
7. Assign a name to the DSL Terminator unit in the System profile.

Configuring an MP or MP+ connection in RADIUS

To configure an MP or MP+ connection in RADIUS, use the attributes listed in Table 4-2.

Table 4-2. MP and MP+ attributes

Attribute	Description	Possible values
Framed-Protocol (7)	Specifies the type of protocol the link can use.	PPP (1) SLIP (2) MPP (256) FR (261) FR-CIR (263) ATM-1483 ATM-FR-CIR By default, the DSL Terminator unit does not restrict the type of protocol a link can use.
Password (2)	Specifies the user's password.	Alphanumeric string of up to 252 characters. The default is null.
User-Name (1)	Specifies the user's name.	Alphanumeric string of up to 252 characters. The default is null.
User-Service (6)	Indicates the framed services that the link can use.	Framed-User (2) Dialout-Framed-User (5) By default, the DSL Terminator unit does not restrict the framed services that a link can use.

To configure an MP or MP+ connection in a RADIUS user profile, follow these steps:

1. On the first line of the profile, specify the User-Name and Password attributes, and set the User-Service parameter to Framed-User.
2. Set the Framed-Protocol parameter to MPP.
3. Set call management attributes. For details, see "Managing bandwidth using RADIUS" on page 5-4.
4. Specify routing or bridging attributes for the connection. For details on specifying that the connection use IP, see Chapter 6, "Configuring IP Routing." For details on specifying protocol-independent bridging, see Chapter 6, "Configuring IP Routing.".
5. Configure the bridging or routing setup in the DSL Terminator unit for the WAN connection. For details, see Chapter 8, "Configuring Packet Bridging".

MP+ connection example

This example shows a user profile for an MP+ link that uses IP routing:

```
John  Password="4yr66", User-Service=Framed-User
          Framed-Protocol=MPP,
          Framed-Address=200.0.5.1,
```

```
Framed-Netmask=255.255.255.0,
Ascend-Route-IP=Route-IP-Yes,
Ascend-Metric=7,
Framed-Routing=None,
Ascend-Idle-Limit=0,
Ascend-Bridge=Bridge-No
```

Setting up a BACP connection

Bandwidth Allocation Control Protocol (BACP) is the Internet standard protocol equivalent to the MP+ protocol. BACP functions similarly to MP+ and uses the same attributes as MP+. The only additional attribute you must set is listed in Table 4-3.

Table 4-3. BACP attribute

Attribute	Description	Possible values
Ascend-BACP-Enable (134)	Specifies whether BACP is enabled on this link.	BACP-No (0) BACP-Yes (1) The default value is BACP-No.

To set up a BACP connection, follow these steps:

1. To enable incoming BACP calls, set the BACP parameter to Yes in Ethernet > Answer > PPP Options.
2. In a RADIUS user profile, set Ascend-BACP-Enable parameter to BACP-Yes.
3. Follow the instructions in “Setting up an MP or MP+ connection using RADIUS” on page 4-24, except for the following:
   - You need not set the MPP parameter to Yes in the Ethernet > Answer > PPP Options menu.
   - You need not set the Framed Protocol parameter to MPP.

Configuring PPP over Ethernet (PPPoE)

PPP over Ethernet (PPPoE) enables a PC to communicate with a Broadband Access Server (such as the DSL Terminator) in order to gain access to a remote network. In general, PPPoE is appropriate for residential, telecommuter, and small- to mid-range customers who want to connect one or more PCs to multiple services at an ISP. The link can use Asynchronous Transfer Mode (ATM), Frame Relay, or PPP.

Point-to-Point Protocol (PPP) is a widely used method for transmitting multiprotocol packets on point-to-point links. To enable users to take advantage of Ethernet’s multipoint support, PPPoE technology allows multiple devices on the Ethernet to initiate PPP sessions with multiple destinations.

The links are created by means of bridging modems. You can connect multiple PCs at a remote site to Customer Premises Equipment (CPE). The CPE can be an Asynchronous Transfer Mode (ATM) bridge that uses RFC-1483 encapsulation, or a Frame Relay bridge that uses RFC-1490 encapsulation. The CPE connects to the DSL Access Multiplexer (DSLAM) at the telephone company's Central Office (CO). The DSLAM then switches the cells or frames across the data network to the DSL Terminator, which terminates the bridged connection. Over this bridged connection, the PC and the DSL Terminator establish a PPP session, which looks like an ordinary dial-up connection to the user. The PC and the DSL Terminator then exchange authentication, accounting, IP address, and other information by means of PPP.

PPPoE works in two basic phases—a Discovery phase and a PPP Session phase. During the Discovery phase, the following events take place:

1 A client that wants to establish a PPPoE session sends a broadcast asking whether any PPPoE services are available.

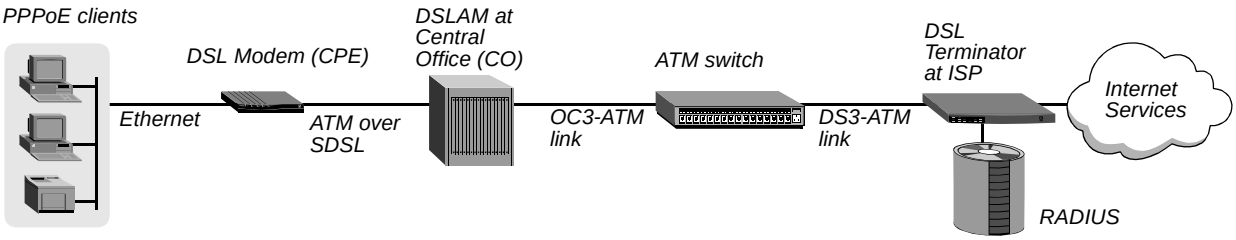
2 The DSL Terminator responds with a packet containing its Ethernet MAC address and verification that it supports PPPoE.

3 The client sends a session-request packet.

4 The DSL Terminator responds with a unique session ID. Together, the MAC address and session ID uniquely identify the PPPoE session.

During the PPP Session phase, the client and the DSL Terminator have sufficient information to create a connection over the Ethernet. The client and the DSL Terminator allocate the resources for the connection, and the client sends PPP packets to the DSL Terminator, just as for an ordinary dial-in session. In Figure 4-3, the PPPoE configuration uses an ATM link.

Figure 4-3. Example of PPPoE configuration



The PPPoE client sends a packet through the DSL modem to the DSLAM. The CO sends the packet through an ATM switch to the DSL Terminator at the ISP. The ISP can then provide the services chosen by the end user.

The DSL Terminator can answer any request from a client requesting a PPPoE connection, provided that:

- PPPoE is enabled on the interface.
- The unit has enough resources to support another session.
- The packets sent by the host are valid according to RFC 2516.

Currently, the DSL Terminator does not provide a way to filter PPPoE packets.

Configuring PPPoE on an Ethernet interface

For the DSL Terminator to respond to PPPoE packets arriving on an Ethernet interface, you must set the PPPoE Enable parameter to Yes in the Ethernet > Mod Config > Ether1 Options or Ether2 Options menu.

Configuring PPPoE over the WAN

To enable a PPPoE client using Asynchronous Transfer Mode (ATM), Frame Relay, or PPP to connect to the DSL Terminator, you must create two Connection profiles—one bridged and one routed. Then, set the LQM parameter to Yes in the Answer profile.

The bridged Connection profile specifies a bridged session between the DSL modem and the DSL Terminator. When the profile is active, the DSL Terminator looks at each PPPoE packet that comes through the interface specified by the bridged profile. The DSL Terminator strips the PPPoE information and passes the packet to the PPP handler. The routed Connection profile then becomes effective.

Creating the bridged Connection profile

Proceed as follows:

1. In the Ethernet > Connections menu, create the Connection profile.
2. Set the Bridge parameter to Yes.
3. Set the Encaps parameter to PPP, FR, or ATM.
4. Navigate to the Ethernet > Connections > PPPoE Options menu.
5. Set the PPPoE Enable parameter to Yes.
6. If you want the unit to bridge packets other than PPPoE for the Connection profile, set the Bridge Non PPPoE parameter to Yes.

Creating the routed Connection profile

Proceed as follows:

1. In the Ethernet > Connections menu, create the Connection profile.
2. Set the Bridge parameter No.
3. Set the Encaps parameter to PPP.
4. Set the Route IP parameter to Yes.

Configuring the LQM setting

In the Ethernet > Answer > PPP Options menu, set the LQM parameter to Yes. With the Yes setting, the unit can detect whether the client has gone offline and stopped responding to LQM packets or Echo Requests.

Understanding PPPoE parameters

This section provides some background about the PPPoE parameters. For detailed information about other parameters, see the *DSL Terminator Reference Guide*.

Parameter	Usage
PPPoE Enable	Specifies whether the unit responds to PPPoE packets arriving on the interface or associated with an active Connection profile. With the Yes setting, the unit responds to PPPoE packets arriving on the interface or associated with the Connection profile. The default setting is No.
Bridge Non PPPoE	Specifies whether the unit bridges packets other than PPPoE for the interface or Connection profile. With the Yes setting, the unit bridges packets other than PPPoE for the interface or Connection profile. The default setting is No.

Settings in a RADIUS profile

Following are the RADIUS attributes for configuring PPP over Ethernet (PPPoE) settings:

- Ascend-PPPoE-Enable
- Ascend-Bridge-Non-PPPoE

Both attributes are available only as Vendor-Specific Attributes (VSAs). VSA functionality must be enabled on the DSL Terminator. For each attribute:

- Length=12
- Vendor-Id=529 (Ascend)
- Vendor-Length=6

PPPoE attribute descriptions

The descriptions that follow provide detailed information about each attribute.

Ascend-PPPoE-Enable (74)	Specifies whether the unit responds to PPPoE packets associated with the user profile. The Ascend-PPPoE-Enable attribute appears in an Access-Accept packet. Specify one of the following values: • PPPoE-Yes (1)—the unit responds to PPPoE packets associated with the user profile. • PPPoE-No (0)—the unit does not respond to PPPoE packets associated with the user profile. Ascend-PPPoE-Enable is not applicable if bridging is turned off for the interface.

Ascend-Bridge-Non-PPPoE (75	Specifies whether the unit bridges packets other than PPPoE for the user profile. The Ascend-Bridge-Non-PPPoE attribute appears in an Access-Accept packet. Ascend-Bridge-Non-PPPoE does not apply if bridging is turned off on the interface, or if Ascend-PPPoE-Enable=PPPoE-No (0). Specify one of the following settings: • Bridge-Non-PPPoE-Yes (1) specifies that the unit bridges packets other than PPPoE for the user profile. • Bridge-Non-PPPoE-No (0) specifies that the unit does not bridge packets other than PPPoE for the user profile.

RADIUS example

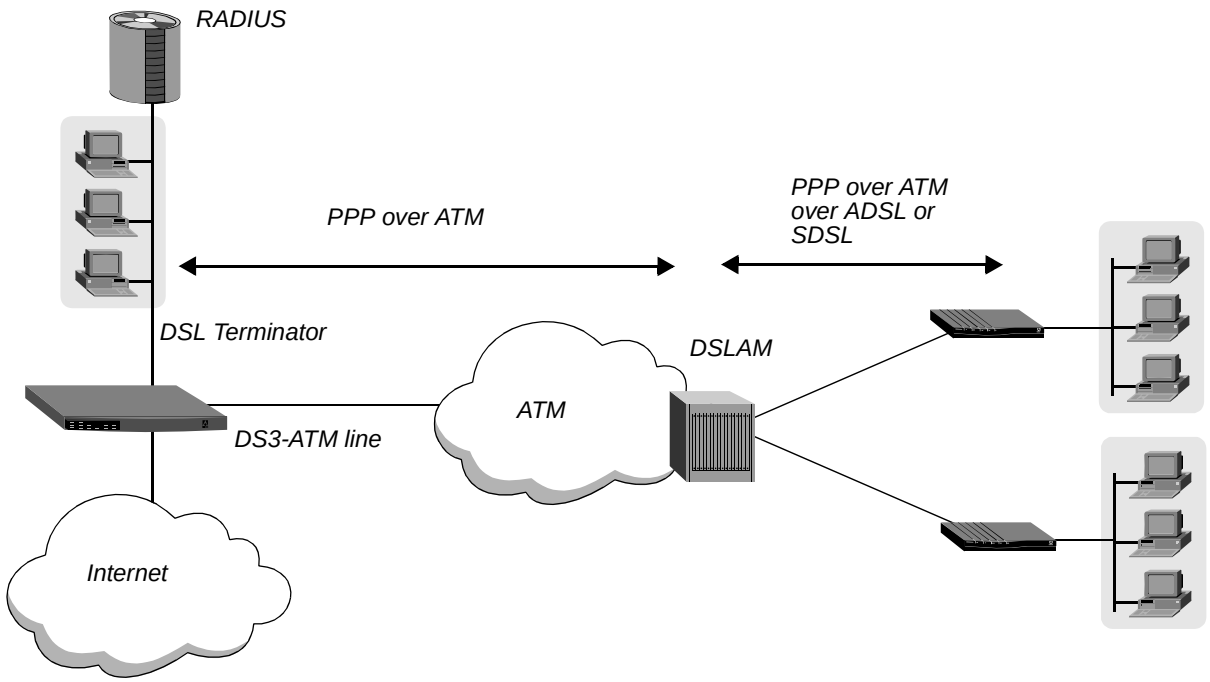
The following user profile specifies that the unit responds to PPPoE packets, and does not bridge packets other than PPPoE:

```
permconn-YossiTerminator-1      Password = "ascend"
          Service-Type = Outbound,
          Framed-Protocol = ATM-1483,
          User-Name = "b-rad-pppoe",
          Framed-Routing = None,
          Ascend-Idle-Limit = 120,
          Acct-Authentic = None,
          Ascend-Send-Auth = Send-Auth-None,
          Ascend-Group = "2",
          Ascend-Call-Type = Nailed,
          Ascend-Route-IP = Route-IP-No,
          Ascend-Bridge = Bridge-Yes,
          Ascend-ATM-Vpi = 15,
          Ascend-ATM-Vci = 35,
          Ascend-Data-Svc = Nailed-64K,
          Ascend-PPPoE-Enable = PPPoE-Yes,
          Ascend-Bridge-Non-PPPoE = Bridge-Non-PPPoE-No
```

Configuring PPP over ATM

The DSL Terminator supports PPP over ATM for incoming virtual connections (VCs) as described in RFC 2364. Encapsulating PPP within ATM enables the DSL Terminator to offer key existing PPP services, such as authentication. Figure 4-4 shows a sample configuration.

Figure 4-4. Example PPP over ATM configuration



When you set up an incoming PPP over an ATM connection, you specify the VPIs and VCIs over which the DSL Terminator will accept incoming PPP connections. The DSL Terminator opens the specified VPIs and VCIs and waits for a connection request.

When a CPE wants to establish a PPP session, it sends a PPP packet to the DSLAM. The DSLAM switches it to an ATM network over a preprovisioned VPI to the DSL Terminator. Once the PPP packet reaches DSL Terminator, the DSL Terminator authenticates the call, determines the VPI/VCI pair the packet came over, and establishes a connection to the CPE over the same VPI/VCI pair.

The DSL Terminator supports PPP over ATM AAL5 with the following restrictions:

- A DS3-ATM or OC3-ATM card is required.
- Only VC-multiplexed PPP is currently supported.
- Only incoming switched PPP over ATM calls are currently supported.

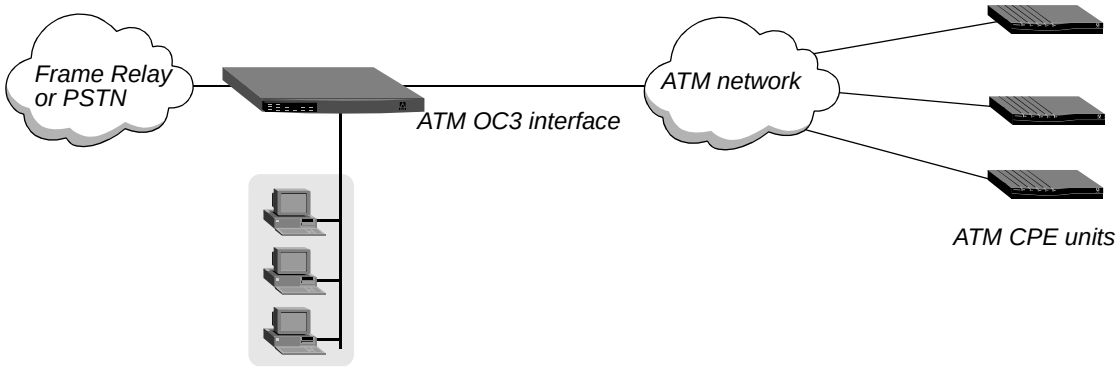
Configuring a PPP over ATM connection

To configure a PPP over ATM connection, proceed as follows:

- Activate the ATM OC3 or DS3 ATM card and specify the incoming VCIs the DSL Terminator will accept.
- Configure a Connection profile on the DSL Terminator (or a RADIUS user profile) for the remote ATM device. The user or site defined by the connection can connect to the DSL Terminator over any of the allowable VPI/VCI pairs configured in the VCC Incoming submenu of the ATM card. and the nailed group configured in the ATM OC3 profile.

Figure 4-5 illustrates an example PPP over ATM connection.

Figure 4-5. Example PPP over ATM configuration



Configuring the ATM card

To configure the ATM card, proceed as in the following example:

1 Open the OC3-ATM profile:

2 Assign a name to the line, if desired:

```
Name=atm-ppp
```

3 Activate the line:

```
Enable=Yes
```

4 Assign a nailed group:

```
Nailed-group=5
```

5 Specify the framing:

```
Framer Rate=STS-3c
```

6 Verify that Loop-Timing is set to its default value of Yes:

```
Loop Timing=Yes
```

7 Specify the VPI/VCI bit range allowed for incoming connections. For example:

```
Vpi/Vci range=0-15/32-4095
```

With this setting, incoming VPIs must range between 0 and 15; incoming VCIs must range between 32 to 4095.

8 Open the Incoming VCCs submenu:

```
10-1** Factory
Incoming VCCs...
 >Incoming Vcc 01
  Incoming Vcc 02
  Incoming Vcc 03
  Incoming Vcc 04
  Incoming Vcc 05
  Incoming Vcc 06
  Incoming Vcc 07
  Incoming Vcc 08
```

9 Open an Incoming VCC profile:

```
  Incoming Vcc 01
 >Enabled = No
  vpi = 0
  Start vci = 32
  End vci = 32
```

10 Enable the VCC submenu:

```
Enabled=Yes
```

11 Specify the VPI and the start and end VCIs that the DSL Terminator will accept for incoming connections. For example:

```
vpi = 12
Start vci = 42
End vci = 46
```

12 Exit and save the profile.

Configuring the Connection profile for the remote device

To configure the Connection profile, proceed as in the following example:

1 Open a Connection profile.

2 Activate the profile:

```
Active=Yes
```

3 Specify PPP encapsulation:

```
Encaps=PPP
```

4 Open the IP Options submenu.

5 Specify the IP address of the remote device. For example:

```
LAN Adrs=192.168.2.1
```

6 Open the Telco Options submenu.

7 Specify the call-type:

```
Call Type=Switched
```

8 Specify the same nailed group number you specified in the Net/OC3-ATM profile:

```
Group=5
```

9 Exit and save the profile.

Configuring Frame Relay

5

Introduction 5-1

Configuring nailed bandwidth for Frame Relay 5-3

Managing bandwidth using RADIUS 5-4

Defining Frame Relay link operations 5-7

Configuring a DLCI logical interface 5-15

Configuring the DSL Terminator as a Frame Relay switch 5-21

Frame Relay and ATM internetworking support 5-30

Introduction

In the Frame Relay network, every access point connects directly to a switch. Frame Relay virtual circuits (VCs) are bidirectional data paths between two end points. An established permanent virtual circuit (PVC) is a connection between two end points, which can include a number of hops in between.

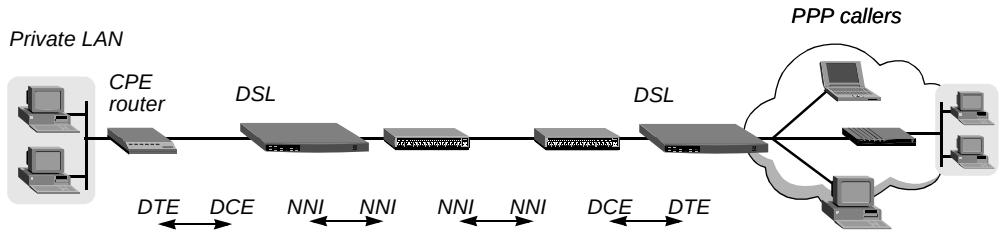
Depending on how a device such as the DSL Terminator is integrated into a Frame Relay network, it can operate as one of the following:

- A Frame Relay terminating unit or customer premise equipment (CPE)
- A Frame Relay switch.

A CPE is the source or destination of data traversing the Frame Relay service. For example, the DSL Terminator labeled DSL Terminator-02 in Figure 5-1 terminates the data stream to its PPP callers. When it is configured with a user-to-network interface (UNI) to Frame Relay, the DSL Terminator acts as the user side (UNI-DTE) communicating with the network side (UNI-DCE) of a switch.

The network-side device connects the CPE device to a Frame Relay network. For example, the DSL Terminator labeled DSL Terminator-01 in Figure 5-1 receives Frame Relay encapsulated frames from a CPE and forwards them on to another Frame Relay switch. When it is configured with a UNI-DCE interface to Frame Relay, the DSL Terminator acts as the network side (UNI-DCE) communicating with the user side (UNI-DTE) of a Frame Relay device.

Figure 5-1. Frame Relay network



A Frame Relay switch is another kind of network-side device that switches frames from one interface to another and exchanges status information with its peer switch. For example, the DSL Terminator labeled DSL Terminator-01 in Figure 5-1 receives frames from its peer switch and switches them to its other Frame Relay interface. When it is configured with a network-to-network interface (NNI) to Frame Relay, the DSL Terminator acts as a Frame Relay switch. Switch-to-switch communication includes both user side (NNI-DTE) and network side (NNI-DCE) functions.

Frame Relay link management

Frame Relay link management enables an administrator to retrieve information about the status of the Frame Relay interface through special management frames with a unique Data Link Connection Identifier (DLCI) address. (DLCI 0 is the default for link management frames.) Link management frames are used to monitor the interface and provide information about DLCI status.

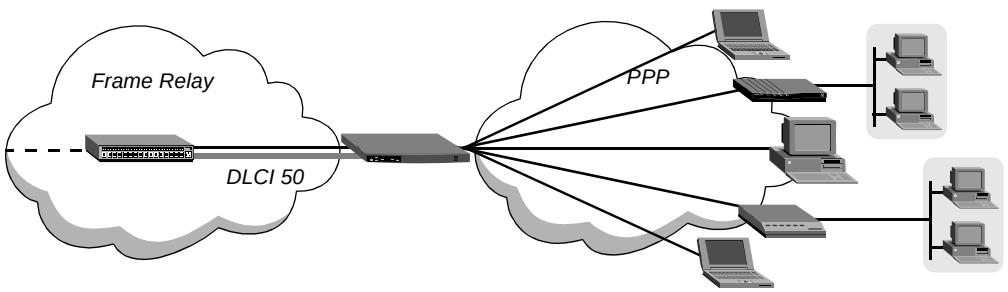
On a UNI interface to Frame Relay, link management procedures occur in one direction. The UNI-DTE device requests information and the UNI-DCE device provides it.

On an NNI interface, link management procedures are bidirectional. Because both sides of the connection request information from their peers, switches perform both the NNI-DTE and NNI-DCE link management functions.

Using the DSL Terminator as a Frame Relay concentrator

As a Frame Relay concentrator, the DSL Terminator forwards many lower-speed PPP connections onto one or more high-speed Frame Relay interfaces, as shown in Figure 5-2:

Figure 5-2. Frame Relay concentrator



In such a configuration, the decision to forward frames onto the Frame Relay interface can be made through OSI layer 3 (routing), or by Frame Relay Direct.

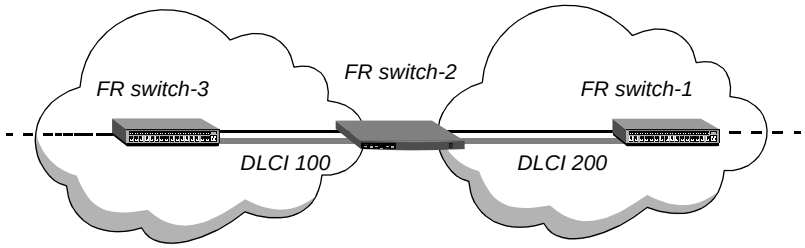
Using the DSL Terminator as a Frame Relay switch

As a Frame Relay switch, the DSL Terminator receives frames on one interface and then transmits them to another interface. The decision to forward frames onto the Frame Relay interface is made through the assignment of circuit names. The DSL Terminator router software is not involved.

To use the DSL Terminator as a switch, configure a circuit that pairs two Frame Relay DLCI interfaces. Instead of going to the layer 3 router for a decision on which interface to forward the frames, it relies on the circuit configuration to relay the frames received on one interface to its paired interface. A circuit is defined in two Connection or RADIUS user profiles.

Figure 5-3 shows the DSL Terminator operating as a Frame Relay switch:

Figure 5-3. Frame Relay switch



Components of a Frame Relay configuration

The physical link to another Frame Relay device must be nailed (similar to a dedicated leased line). You can allocate nailed bandwidth in a line profile (the profile of a T1, E1, SWAN, or other network line).

The link interface to the Frame Relay device, which is also called a datalink, references specific nailed bandwidth in the DSL Terminator and defines the operations and link management functions that the DSL Terminator performs on the interface. You can specify these settings in a Frame Relay profile or RADIUS frdlink pseudo-user profile.

The logical interface is a PVC end point, which requires a DLCI. DLCIs uniquely identify the logical end points of a virtual circuit (a specific end device). Obtain DLCIs from your Frame Relay provider and assign them in Connection profiles or RADIUS user profiles.

Configuring nailed bandwidth for Frame Relay

Each Frame Relay interface in the DSL Terminator requires its own nailed bandwidth, which is similar to a dedicated leased line.

Note: If you configure the bandwidth on a nailed T1 line, make sure that the number of channels that the DSL Terminator uses for the link matches the number of channels used by the

device at the other end of the link and that only one line profile specifies the Nailed-Group number to be used by the Frame Relay datalink.

Following are some examples of relevant parameters, shown with sample settings:

```
Net/T1 > Line Config > Line 1 > Ch 2=Nailed
Net/T1 > Line Config > Line 1 > Ch 2 Prt/Grp=1
Net/E1 > Line Config > Line 1 > Ch 2=Nailed
Net/E1 > Line Config > Line 1 > Ch 2 Prt/Grp=1
Serial WAN > Mod Config > Nailed Grp=1
```

Parameter	Specifies
Ch *N*	Switched or Nailed channel usage. To configure nailed bandwidth on a channelized T1 or E1 card, select Nailed-64-Channel (a clear-channel 64K circuit). On unchannelized cards, this parameter does not apply.
Ch *N* Prt/Grp Nailed Grp	An integer from 1 to 1024 that is used to identify nailed bandwidth. Frame Relay profiles or RADIUS frdlink pseudo-user profiles specify this number to use the associated bandwidth.

For more details about configuring T1, see the *DSL Terminator Hardware Installation Guide*.

Managing bandwidth using RADIUS

You can manage bandwidth by specifying a time limit for a session and the DSL Terminator's response to an idle connection. To manage bandwidth in RADIUS, use the attributes listed in Table 5-1.

Table 5-1. Bandwidth management attributes

Attribute	Description	Possible values
Ascend-Idle-Limit (244)	Specifies the number of seconds the DSL Terminator waits before clearing a call when a session is inactive.	Integer between 0 and 65535. The default value is 120. If you accept the default setting and the Answer profile specifies a value for the analogous Idle parameter, the DSL Terminator ignores the Idle value and uses the Ascend-Idle-Limit default.
Ascend-Maximum-Call-Duration (125)	Specifies the maximum number of minutes an incoming call can remain connected.	Integer between 0 and 1440. The default value is 0 (zero).

Table 5-1. Bandwidth management attributes (continued)

Attribute	Description	Possible values
Ascend-Maximum-Time (194)	Specifies the maximum length of time in seconds that any session can remain online. Once a session reaches the time limit, the DSL Terminator takes its connection offline.	Integer between 0 and 4,294,967,295. The default value is 0 (zero). When you accept the default setting, the DSL Terminator does not enforce a time limit.

To manage bandwidth, follow these steps:

1 Configure an MP+ connection, as described in "Setting up an MP or MP+ connection using RADIUS" on page 4-24.

2 To specify the maximum number of minutes that an incoming call can remain connected, set the Ascend-Maximum-Call-Duration attribute. The DSL Terminator checks the connection once per minute, so the actual time the call remains connected is slightly longer than the actual time you set.

3 To specify the maximum length of time in seconds that the DSL Terminator allows any session to stay online, set the Ascend-Maximum-Time attribute. Once a session reaches the time limit, the DSL Terminator takes its connection offline.

4 To indicate the number of seconds the DSL Terminator waits before clearing a call when a session is inactive, set the Ascend-Idle-Limit attribute. If you specify 0 (zero), the DSL Terminator always clears a call when a session is inactive. The Ascend-Idle-Limit attribute does not apply to nailed-up links.

Setting up a nailed-up connection using RADIUS

A nailed-up connection is a permanent link that is always up as long as the physical connection persists. If the unit or central switch resets or if the link goes down, the DSL Terminator attempts to restore the link at 10-second intervals. If the DSL Terminator or the remote unit is powered off, the link comes back up when the device is plugged in again.

Before configuring a nailed-up connection in a RADIUS user profile, perform the following tasks in the DSL Terminator configuration interface:

1 In the Line profile, specify which channels are nailed-up. For example, if Channel 2 is nailed-up, specify this setting:

```
Ch 2=Nailed
```

Nailed specifies that the channel is permanently connected. No dialout is required, so nailed-up channels do not require a phone number.

2 For each nailed-up channel, specify a group number from 1 to the maximum number of nailed groups that the DSL Terminator allows. For example, to assign Channel 2 to Group 9, make this specification:

```
Ch 2 Prt/Grp=9
```

Configuring a nailed-up connection in RADIUS

To configure a nailed-up connection in RADIUS, use the attributes listed in Table 5-2.

Table 5-2. Nailed-up attributes

Attribute	Description	Possible values
Ascend-backup (176)	Specifies the name of a backup profile for a nailed link whose physical connection fails.	Text string. The default is null.
Ascend-Group (178)	Points to the nailed-up channels that the WAN link uses.	Single integer between 1 and 60. The default value is 1.
Framed-Protocol (7)	Specifies the type of protocol the link can use.	PPP (1) MPP (256) FR (261) FR-CIR (263) ATM-1483 ATM-FR-CIR By default, the unit does not limit the protocols a link can use.
Password (2)	Specifies the user's password.	Alphanumeric string of up to 252 characters. The default is null.
User-Name (1)	Specifies the user's name.	Alphanumeric string of up to 252 characters. The default is null.
User-Service (6)	Indicates the type of framed services the link can use.	Framed-User (2) Dialout-Framed-User (5) By default, the DSL Terminator does not restrict the framed services that a link can use.

To configure a nailed-up connection in a RADIUS user profile, follow these steps:

1 On the first line of the RADIUS user profile, specify the User-Name, Password, and User-Service attributes.

- For the User-Name attribute, specify a name that indicates an outgoing nailed-up connection.
- Set Password= "Ascend".
- Set User-Service=Dialout-Framed-User: This setting ensures that the DSL Terminator cannot use the profile for authentication of an incoming call.

For example, you might enter this first line in the profile:

```
Permconn-Unit2 Password="Ascend", User-Service=
Dialout-Framed-User
```

2 On the second line of the user profile, specify the User-Name attribute to indicate the name of the user that can make the nailed-up connection.

3 Set the Framed-Protocol attribute.

4 To specify the nailed-up channels the profile can use, set the Ascend-Group attribute.

This attribute points to the nailed-up channels that the WAN link uses. Specify a number between 1 and 60. The default value is 1.

Nailed-up connection example

The pseudo-user profile in this example defines a nailed-up PPP connection using group number 2:

```
Permconn-Unit2 Password="Ascend", User-Service=Dialout-Framed-User
       User-Name="Matt",
       Framed-Protocol=PPP,
       Framed-Address=50.1.1.1,
       Framed-Netmask=255.0.0.0,
       Ascend-Route-IP=Route-IP-Yes,
       Ascend-Metric=7,
       Framed-Routing=None,
       Ascend-Idle-Limit=0,
       Ascend-Bridge=Bridge-No,
       Ascend-Group="2"
```

Modifying or deleting nailed-up profiles

To modify or delete nailed-up profiles, follow these steps:

1 Change or delete the profile on the RADIUS server.

2 Choose the Upd Rem Cfg command from the Sys Diag menu.

The DSL Terminator closes all the sessions related to all nailed-up profiles, deletes all the profiles from the system, and restarts the process of retrieving profiles from RADIUS.

Defining Frame Relay link operations

A Frame Relay profile defines datalink operations, including link management functions. The same settings can be specified in a RADIUS frdlink pseudo-user profile.

Note: Link management settings are optional. It is possible to set up a Frame Relay interface and pass data across it without setting these parameters. However, link management parameters provide a mechanism for retrieving information about the status of the interface and its DLCIs.

Understanding Frame Relay parameters

Following are the Frame Relay profile parameters, shown with sample settings:

```
Ethernet
   Frame Relay
      Name*=""
      Active=Yes
      Call Type=Nailed
      FR Type=NNI
```

```
Nailed Grp=1
Data Svc=56KR
PRI # Type=N/A
Dial #=N/A
Bill #=N/A
Call-by-Call=N/A
Transit #=N/A
Link Status Dlci=0
Link Mgmt=T1.617D
N391=6
DTE N392=3
DTE N393=4
DCE N392=3
DCE N393=4
T391=10
T392=15
MRU=1532
```

These parameters are in Ethernet>Frame Relay > *Frame Relay profile.* For detailed information about each parameters, see the *DSL Terminator Reference*.

Parameter	Description
Name	Unique name of the Frame Relay profile (up to 15 characters). The Frame Relay name referenced in user profiles that make use of this datalink.
Active	Set the Active parameter to Yes to activate the profile.
Call Type	Specifies the type of connection. Select Nailed or Switched. If set to Nailed, the Dial# and Bill# parameters do not apply. If set to Switched, the Nailed Grp parameter does not apply.
FR Type	Specify one of the following frame relay types: • NNI —NNI interface to the switch • DCE—UNI-DCE interface • DTE—UNI-DTE interface
Nailed Grp	Group number assigned to nailed channels in a line profile, such as a T1 or E1 profile. The default value is 1. If the channels are on a nailed T1 line, make sure that the number of channels used by the devices at both end of the link match and that only one T1 profile specifies the number to be used by the Frame Relay data link.
Data Svc	The bandwidth of data service provided over a WAN line. A data service can transmit either data or digitized voice. Specify 64K or 56K. Usually set to 64k for a Frame Relay datalink.
PRI # Type	Specifies the TypeOfNumber field in the called party's information element. 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 information on what setting to use.

Parameter	Description
Bill #	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.
Call-by-Call	Signaling value that the PRI service uses when placing a call using that profile.
Transit #	Dialing prefix 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.
Link Mgmt	Link management protocol to use between the DSL Terminator and the Frame Relay switch. Obtain this value from your Frame Relay provider. Specify one of the following values for the Link management protocol: • None—no link management • T1.617D—T1.617 Annex D • Q.933A—Q.933 Annex A
N391	Interval at which the DSL Terminator requests a Full Status Report (from 1 to 255 seconds). Does not apply if FR Type is set to DCE.
DCE N392	Number of errors during DCE N393 monitored events that causes the network side to declare the user-side procedures inactive. The value should be less than that of DCE N393 (from 1 to 10). Does not apply if FR Type is DTE.
DCE N393	Specifies the DCE monitored event count (from 1 to 10). Does not apply if FR Type is DTE.
DTE N392	Specifies the number of errors, during DTE N393 monitored events, that cause the user side to declare the network-side procedures inactive. The value should be less than that of DTE N393 (from 1 to 10). Does not apply if FR Type is DCE.
DTE N393	Specifies the number of DTE monitored events per testing cycle (from 1 to 10). Does not apply if FR Type is DCE.
T391	Specifies the Link Integrity Verification polling timer (from 5 to 30 seconds). The value should be less than that of T392. T391 is N/A when FR Type is DCE.
T392	Specifies the interval for Status Enquiry messages (from 5 to 30 seconds). The DSL Terminator records an error message if it does not receive an Status Enquiry message within T392 seconds. Does not apply if FR Type is DTE.
MRU	Specifies the Maximum Receive Units (MRUs) value which is the maximum number of bytes the DSL Terminator can receive in a single packet across this link. Leave this parameter at its default of 1532 unless the far end device requires a lower number.
MFR Bundle Name	Specifies the name of a multilink Frame Relay bundle. This parameter adds the data link and all DLCIs that use it to the MFR bundle. All member data links must specify the same bundle name in the Frame-Relay profile.Specify the name of a Multi-Link-FR profile. Specify a name of up to 15 characters that is unique system-wide.

Settings in a RADIUS frdlink profile

An frdlink profile is a pseudo-user profile in which the first line has this format:

`frdlink-`*`name`*`-N Password="ascend", User-Service = Dialout-Framed-User`

The *name* argument is the DSL Terminator system name (specified by the Name parameter in the System profile), and *N* is a number in a sequential series, starting with 1. Make sure there are no missing numbers in the series specified by *N*. If there is a gap in the sequence of numbers, the DSL Terminator stops retrieving the profiles.

The following attributes can be used to define a frdlink pseudo-user profile:

Attribute	Value
Ascend-FR-Profile-Name (180)	A Frame Relay profile name (up to 15 characters), to be referenced in user profiles that make use of this datalink.
Ascend-FR-Nailed-Grp (158)	Group number assigned to nailed bandwidth in a line profile, such as a T1 or E1 profile. The default is 1. Make sure the Frame Relay profile specifies the correct group number. If the channels are on nailed T1 connection, make sure that the number of channels that the DSL Terminator uses for the link matches the number of channels used by the device at the other end of the link, and that only one T1 profile specifies the Nailed-Group number to be used by the Frame Relay datalink.
Ascend-Call-Type (177)	Type of nailed connection: • Nailed (1) (Default) • Nailed/Mpp (2) • Perm/Switched (3).
Ascend-Data-Svc (247)	Type of data service on the nailed link.Typically set to Nailed-64K for a Frame Relay datalink.
Ascend-FR-Link-Mgt (160)	The link management protocol. Specify one of the following: • Ascend-FR-No-Link-Mgt (0)—link management protocol is disabled. This is the default. • Ascend-FR-T1-617D (1)—Annex D. • Ascend-FR-Q-933A (2)—CCITT Q.933 Annex A Ascend-FR-No-Link-Mgt is the default. To ensure interoperability with equipment from different vendors, use the same version of management protocol at each end of the Frame Relay link.

Attribute	Value
Ascend-FR-Type (159)	Type of operations performed by the DSL Terminator on this interface. Settings are: • Ascend-FR-DTE (0) (Default) • Ascend-FR-DCE (1) • Ascend-FR-NNI (2). For more information, see “Examples of a UNI-DTE link interface” on page 5-12, “Examples of a UNI-DCE link interface” on page 5-13, and “Examples of an NNI link interface” on page 5-14.)
Ascend-FR-N391 (161)	Number of T391 polling cycles between full Status Enquiry messages. The default value ,6, indicates that after 6 status requests (spaced Ascend-FR-T391 seconds apart), the UNI-DTE device requests for a full status report. Does not apply when Ascend-FR-Type is Ascend-FR-DCE.
Ascend-FR-DTE-N392 (163)	Number of errors which, if occurring in the number of DTE monitored events specified by Ascend-FR-DTE-N393, causes the user-side to declare the network-side procedures inactive. Specify a value that is less than that of Ascend-FR-DTE-N393l (which can be from 1 to 10). The default value is 3. Does not apply when Ascend-FR-Type is Ascend-FR-DCE.
Ascend-FR-DTE-N393 (165)	DTE monitored event count (from 1 to 10). The default is 4. Does not apply when Ascend-FR-Type is Ascend-FR-DCE.
Ascend-FR-T391 (166)	Link Integrity Verification polling timer. Specify a value that is less than that of Ascend-FR-T392. The default value, 10, indicates that after Ascend-FR-N391 status requests spaced 10 seconds apart, the UNI-DTE device requests a Full status report. Does not apply when Ascend-FR-Type is Ascend-FR-DCE.
Ascend-FR-T392 (167)	Interval during which Status Enquiry messages should be received (from 5 to 30 seconds). The default T392 value is 15. An error is recorded if no Status Enquiry is received within the specified number seconds. Does not apply when Ascend-FR-Type is Ascend-FR-DTE.
Framed-MTU (12)	Maximum number of bytes the that DSL Terminator can transmit in a single packet across the link interface. Usually, the default value of 1532 is the right setting. However, the far end device might require a lower number.
Ascend-FR-DCE-N392 (162)	Number of errors which, if occurring in the number of DCE monitored events specified by Ascend-FR-DCE-N393, causes the network-side to declare the user-side procedures inactive. Specify a value that is less than that of Ascend-FR-DCE-N393 (which can be from 1 to 10). Does not apply when Ascend-FR-Type is Ascend-FR-DTE.
Ascend-FR-DCE-N393 (164)	DCE monitored event count (from 1 to 10). The default is 4. Does not apply when Ascend-FR-Type is Ascend-FR-DTE.

Attribute	Value
Ascend-FR-Link-Status-Dlci (106)	DLCI to use for LMI link management on the Frame Relay datalink. Valid values are DLCI0 (the default) and DLCI1023.

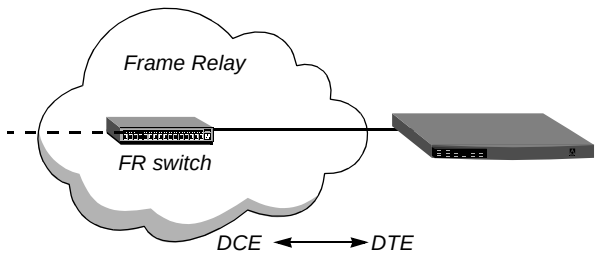
Examples of a UNI-DTE link interface

On a UNI-DTE interface, the DSL Terminator acts as the user side communicating with the network side DCE switch. It initiates link management functions by sending a Status Enquiry to the UNI-DCE device. Status Enquiries can include queries about the status of PVC segments the DTE knows about, as well as the integrity of the datalink between the UNI-DTE and UNI-DCE interfaces.

The UNI-DTE uses the values of the N391, N392, N393, and T391 parameters in the Frame Relay profile to define the timing of its Status Enquiries to the DCE and its link integrity parameters. (These correspond to the Ascend-FR-N391, Ascend-FR-DTE-N392, Ascend-FR-DTE-N393, and Ascend-FR-T391 attributes in a RADIUS profile.)

Figure 5-4 shows an example of the DSL Terminator with a UNI-DTE interface.

Figure 5-4. Frame Relay DTE interface



The following parameters specify nailed group 11 as the bandwidth for the sample DTE interface. *Make sure that the Frame Relay profile specifies the correct nailed group.*

```
Ethernet
   Frame Relay
      Active=Yes
      FR Type=DTE
      Nailed Grp=11
      Link Mgmt=Q.933A
```

In the preceding link management settings, the DSL Terminator uses the CCITT Q.933 Annex A link management protocol to communicate with the Frame Relay DCE. It initiates link management functions by sending a Status Enquiry to the DCE every 10 seconds.

On a UNI-DTE interface, the state of a DLCI is determined by the Full status report from the DCE or by an async PVC update. The Full status report from the DCE specifies active and inactive and new DLCIs. If the DCE does not specify a DLCI as active or inactive, the DTE considers it inactive.

Following is a comparable RADIUS profile:

```
frdlink-max-1 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "fr-dte",
```

```
Ascend-Call-Type = Nailed,
Ascend-FR-Type = Ascend-FR-DTE,
Ascend-FR-Nailed-Grp = 11,
Ascend-FR-Link-Mgt = Ascend-FR-Q-933A,
Ascend-Data-Svc = Nailed-64K
```

Examples of a UNI-DCE link interface

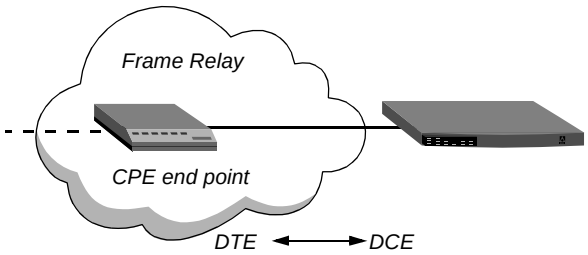
On a UNI-DCE interface, the DSL Terminator acts as the network side communicating with the user side (UN-DTE) of a Frame Relay terminating unit.

The UNI-DCE uses the values of the T392, DCE N392, and DCE N393 parameters in the Frame Relay profile to define the parameters of the Status Enquiries expected from the DTE. (These values correspond to the Ascend-FR-T392, Ascend-FR-DCE-N392, and Ascend-FR-DCE-N393 attributes in a RADIUS profile.)

For example, if the DSL Terminator expects a Status Enquiry from the DTE every ten seconds, it records an error if it does not receive a Status Enquiry in ten seconds.

Figure 5-5 shows an example of the DSL Terminator with a UNI-DCE interface.

Figure 5-5. Frame Relay DCE interface



The following parameters specify nailed group 36 as the bandwidth for the sample DCE interface. *Make sure that the Frame Relay profile specifies the correct nailed group.*

```
Ethernet
   Frame Relay
      Active=Yes
      FR Type=DCE
      Nailed Grp=36
      Link Mgmt=Q.933A
      T392=15
```

In the preceding link management settings, the DSL Terminator uses the CCITT Q.933 Annex A link management protocol to communicate with the CPE end point. It expects a Status Enquiry at intervals less than seven seconds.

On a UNI-DCE interface, if the datalink is up, the DLCI is considered to be up as well. In the DCE Full status response to the DTE, if a PVC segment terminates within the DCE, it is reported as active. If the PVC segment is not terminated, the DCE has to request further information on the Frame Relay network. In that case, it requests information about the DLCI

from the next hop switch, and reports back to the DTE when the segment is confirmed to be active or inactive.

Following is a comparable RADIUS profile:

```
frdlink-max-2 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "fr-dce",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DCE,
    Ascend-FR-Nailed-Grp = 36,
    Ascend-FR-Link-Mgt = Ascend-FR-Q-933A,
    Ascend-Data-Svc = Nailed-64K,
    Ascend-FR-T392 = 15
```

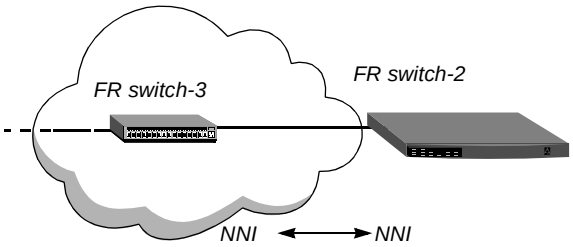
Examples of an NNI link interface

An NNI interface implements procedures used by Frame Relay switches to communicate status between them. The DSL Terminator uses these procedures to inform its peer switch about the status of PVC segments from its side of the Frame Relay network, as well as the integrity of the datalink between them. The procedure is bidirectional. The switches act as both the user side (DTE) and network side(DCE) in that they both send Status Enquiries and respond to them.

Because NNI is bidirectional, all of the link management values defined in the Frame Relay profile are used. The values of the N391, N392, N393, and T391 parameters define the user side of the NNI. These values define the timing of the status enquiries the DSL Terminator sends to its peer switch and the boundary conditions that define link integrity. The values of the T392l, DCE N392, and DCE N393 parameters are used by the network side of the NNI to define the parameters of the Status Enquiries it expects from the its peer switch.

Figure 5-6 shows a DSL Terminator with an NNI interface.

Figure 5-6. Frame Relay NNI interface



To operate as a switch, the DSL Terminator requires a hard-coded circuit configuration in two Connection profiles. It relies on the circuit configuration to relay the frames received on one of the circuit end points to the other circuit end point. For details about circuit configuration, see “Configuring the DSL Terminator as a Frame Relay switch” on page 5-21.

Note: The two Frame Relay end points that make up the circuit do not require NNI interfaces.

The following parameters specify the nailed group 52 as the bandwidth for the NNI interface to Switch-3 (Figure 5-6). *Make sure that the Frame Relay profile specifies the correct nailed group.*

```
Ethernet
   Frame Relay
      Active=Yes
      FR Type=NNI
      Nailed Grp=52
      Link Mgmt=T1.617D
      N391=6
      T391=10
      T392=15
```

In the preceding link management settings, the DSL Terminator uses the ANSI Annex D link management protocol to communicate with Switch-3. It sends a Status Enquiry for Link Integrity Verification to Switch-3 every 10 seconds, and requests a Full status report every sixth enquiry (every 60 seconds). It also sends a Full Status report in response to requests from the other switch. If it does not receive a Status Enquiry within a 15-second interval (T392), it records an error.

Following is a comparable RADIUS profile:

```
frdlink-max-3 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "switch-3",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-NNI,
    Ascend-FR-Nailed-Grp = 52,
    Ascend-FR-Link-Mgt = Ascend-FR-T1-617D,
    Ascend-Data-Svc = Nailed-64K,
    Ascend-FR-N391 = 6,
    Ascend-FR-T391 = 10,
    Ascend-FR-T392 = 15
```

Configuring a DLCI logical interface

A Connection profile defines a DLCI interface. The same settings can be specified in a RADIUS permconn pseudo-user profile.

Overview of DLCI interface settings

You can configure a Connection or RADIUS permconn profile that specifies a connection to a far end device across Frame Relay. The first hop of the connection is known by the DLCI assigned in the profile.

A DLCI is an integer between 16 and 991 that uniquely identifies a specific end point in the Frame Relay network. Obtain a valid DLCI for each logical interface to a Frame Relay network from you Frame Relay service provider.

Settings in a Connection profile

All connections that use Frame Relay must specify the name of a configured Frame Relay profile that defines the data link between the DSL Terminator and the Frame Relay network.

Forwarded or routed connections over the Frame Relay link use the following sets of parameters (shown with sample settings):

```
Ethernet
   Answer
      Encaps...
         PPP=Yes
         FR=Yes

      PPP Options...
         Route IP=Yes
```

For gateway connections:

```
Ethernet
   Connections
      any Connection profile
         Encaps=FR
         Encaps options...
            FR Prof=pacbell
            DLCI=16
            Circuit=N/A

         Route IP=Yes

         Ip options...
         LAN Adrs=10.2.3.4/24
```

For Frame Relay circuits:

```
Ethernet
   Connections
      any Connection profile
         Encaps=FR_CIR
         Encaps options...
            FR Prof=pacbell
            DLCI=16
            Circuit=circuit-1
```

For FR Direct connections:

```
Ethernet
   Connections
      any Connection profile
         Encaps=PPP
         Route IP=Yes
         Ip options...
            LAN Adrs=10.2.3.4/24

         Session options...
            FR Direct=Yes
            FR Prof=pacbell
            DLCI=16
```

Understanding the Frame Relay connection parameters

This section provides some background information about the Frame Relay connection parameters. For detailed information about each parameter, see the *TAOS RADIUS Guide*.

Tyoe of connections	**Description**
Gateway connections	Gateway connections require that the Encaps parameter is set to FR, a Frame Relay profile name, and a DLCI. Ask you Frame Relay provider for the DLCI value to assign to each connection. A Connection profile that specifies Frame Relay encapsulation must include a DLCI to identify the first hop of a permanent virtual circuit (PVC). Do not enter duplicate DLCIs, except when they are carried by separate physical links specified in different Frame Relay profiles.
Frame Relay circuits	A circuit is a PVC segment configured in two Connection profiles. Data coming in on the DLCI configured in one Connection profile is switched to the DLCI configured in the other. Data gets dropped if the circuit has only one DLCI. If more than two Connection profiles specify the same circuit name, the DSL Terminator uses only two DLCIs. In a circuit, both Connection profiles must specify FR_CIR encapsulation (the Encaps parameter is set to FR_CIR) and the same circuit name. Each profile must specify a unique DLCI. The DSL Terminator does not allow you to enter duplicate DLCIs, except when separate physical links specified in different Frame Relay profiles carry duplicate DLCIs.
FR Direct connections	In an FR Direct connection, the DSL Terminator simply *attaches* a Frame Relay PVC to multiple Connection profiles. It does so in the Session Options subprofile, by enabling FR Direct, specifying a Frame Relay profile, and setting a DLCI for the PVC end point in the FR DLCI parameter. Any packet coming into the DSL Terminator on these connections is switched out on the DLCI. In this mode, the DSL Terminator allows multiple Connection profiles to specify the same PVC (the same DLCI). FR Direct is an unusual mode in that the DSL Terminator ignores the destination of the packets. It assumes that some device at the far end of the PVC makes the routing decisions. The Connection profile, however, must use IP routing to enable the DSL Terminator to route data back to the client.

Settings in a RADIUS profile

A permconn profile is a pseudo-user profile in which the first line has this format:

`permconn-`*`name`*`-N Password="ascend", User-Service = Dialout-Framed-User`

The *name* argument is the DSL Terminator system name (specified by the Name parameter in the System profile), and *N* is a number in a sequential series, starting with 1. Make sure there are no missing numbers in the series specified by *N*. If there is a gap in the sequence of numbers, the DSL Terminator stops retrieving the profiles when it encounters the gap in sequence.

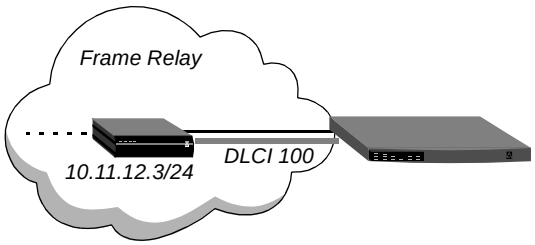
The following attributes can be used to define a permconn pseudo-user profile that uses Frame Relay:

Attribute	Value
User-Name (1)	Name of the far end Frame Relay device.
Framed-Protocol (7)	Encapsulation protocol. Must be set to FR (261).
Ascend-FR-Profile-Name (180)	Name of the Frame Relay profile that defines the data link.
Ascend-FR-DLCI (179)	A DLCI for this PVC end point. Obtain the DLCI from your Frame Relay provider. The DSL Terminator does not allow you to enter duplicate DLCIs, except when they are carried by separate physical links specified in different Frame Relay profiles.
Ascend-Backup (176)	Name of a backup Connection profile to the next hop (optional). See "Examples of backup interfaces for nailed Frame Relay links" on page 5-19.

Examples of a DLCI interface configuration

In the following example, the DSL Terminator has a connection to a Frame Relay switch that also supports IP routing, as shown in Figure 5-7:

Figure 5-7. Frame Relay PVC



The following set of parameters configures the Connection profile, assigning DLCI 100:

```
Ethernet
   Connections
      any Connection profile
         Active=Yes
         Encaps=FR
         IP options
            LAN Adrs=10.11.12.3/24
         Encaps options
            FR Prof=fr-dce
            DLCI=100
```

```
         Telco options
            Call Type=Nailed
```

Following is a comparable RADIUS profile:

```
permconn-max-1 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "max-switch",
    Framed-Protocol = FR,
    Framed-Address = 10.11.12.3,
    Framed-Netmask = 255.255.255.0,
    Ascend-Route-IP = Route-IP-Yes,
    Ascend-FR-DLCI = 100,
    Ascend-FR-Profile-Name = "fr-dce"
```

Note: When IP routing is enabled, the DSL Terminator creates a route for this destination. You can choose to add static routes to other subnets or to enable RIP updates to or from the router across Frame Relay. The usual considerations for IP routing connections apply (see Chapter 6, “Configuring IP Routing”).

Examples of backup interfaces for nailed Frame Relay links

On UNI-DTE and NNI interfaces, the DSL Terminator issues Status Enquiries that check the state of the other end of PVC segments on the interface. If a DLCI becomes inactive and the profile configuring its nailed interface specifies a backup connection, the DSL Terminator uses the backup connection to provide an alternate route to the other end. For an introduction to backup interfaces, see “Examples of backup interfaces for nailed Frame Relay links” on page 5-19.

In the sample profiles that follow, the primary interface is a Frame Relay DLCI interface defined in a profile named `fp7` and the backup interface is another DLCI interface defined in a profile named `pvc`. In this example, the remote IP address of the primary and the backup connection are different.

The following set of parameters defines the primary and backup interfaces in local Connection profiles:

```
Ethernet
   Connections
      fp7
         Name=fp7
         Active=Yes
         Encaps=FR
         IP options
            LAN Adrs=10.168.7.9/24
         Encaps options
            FR Prof=frt2-7
            DLCI=18
         Telco options
            Call Type=Nailed
         Session options
            BackUp=pvc

Ethernet
```

```
Connections
   pvc
      Name=pvc
      Active=Yes
      Encaps=FR
      IP options
         LAN Adrs=10.168.7.11/24
      Encaps options
         FR Prof=frt1-7
         DLCI=16
      Telco options
         Call Type=Nailed
```

Following are comparable RADIUS profiles:

```
permconn-max1-1 Password = "ascend", User-Service = Dialout-Framed-
User
   User-Name = "fp7",
   Framed-Protocol = FR,
   Framed-Address = 10.168.7.9,
   Framed-Netmask = 255.255.255.0,
   Ascend-Route-IP = Route-IP-Yes,
   Ascend-Backup = "pvc",
   Ascend-Metric = 7,
   Ascend-FR-DLCI = 18,
   Ascend-FR-Profile-Name = "radius-frt2-7",
   Framed-MTU = 1524,
   Ascend-Call-Type = Nailed

permconn-max1-2 Password = "ascend", User-Service = Dialout-Framed-
User
   User-Name = "pvc",
   Framed-Protocol = FR,
   Framed-Address = 10.168.7.11,
   Framed-Netmask = 255.255.255.0,
   Ascend-Route-IP = Route-IP-Yes,
   Ascend-Metric = 7,
   Ascend-FR-DLCI = 16,
   Ascend-FR-Profile-Name = "radius-frt1-7",
   Framed-MTU = 1524,
   Ascend-Call-Type = Nailed
```

When the DSL Terminator brings up the two Frame Relay PVC, the routing table includes entries such as this:

```
...

10.168.7.0/24    10.168.7.9     wan33     rGT     60    1     0    89
10.168.7.0/24    10.168.7.9     wan33     *SG    120    7     0   198
10.168.7.9/32    10.168.7.9     wan33     rT      60    1     0    89
10.168.7.9/32    10.168.7.9     wan33     *      120    7         198
10.168.7.11/32   10.168.7.11    wan32     rT      60    1     0    51
10.168.7.11/32   10.168.7.11    wan33     *S     120    1          89
...
```

At this point, both nailed connections are up, and the output of the Ifmgr command contains entries such as the following:

```
bif slot sif u m p ifname   host-name remote-addr      local-addr
-------------------------------------------------------------------
032 1:03 001 *   p wan32    pvc       10.168.7.11/32   11.168.6.234/32
033 1:03 002 *   p wan33    fp7       10.168.7.9/32    11.168.6.234/32
```

If the primary PVC becomes unavailable, the routing table does not change, but the entries in the output of the Ifmgr command look like the following output:

```
bif slot sif u m p ifname  host-name  remote-addr      local-addr
-------------------------------------------------------------------
032 1:03 001 *   p wan32    pvc       10.168.7.11/32   11.168.6.234/32
033 1:17 000 +   p wan33    fp7       10.168.7.9/32    11.168.6.234/32
```

Notice that `fp7` is shown with a plus-sign (+) to show that it is in the Backup Active state (that it is backed up by another connection). When the primary PVC comes up again, the data flow is directed to that interface again. At that point, the Ifmgr command output again shows both interfaces as up.

Configuring the DSL Terminator as a Frame Relay switch

As a Frame Relay switch, the DSL Terminator receives frames on one DLCI interface and transmits them on another one. The decision to forward frames is made on the basis of circuit name assignments.

To use the DSL Terminator as a switch, you must configure a circuit that pairs two DLCI interfaces. Instead of going to the Layer 3 router for a decision on which interface to forward the frames, it relies on the circuit name to relay the frames to the paired interface. A circuit is defined in two Connection profiles, one for each end point of the circuit.

Note: When it is operating as a switch, the DSL Terminator relays all frames received on one end point of the circuit to the other end point of the circuit. It does not examine the packets at Layer 3.

Overview of circuit-switching parameters

With a Frame Relay circuit configuration, the DSL Terminator can operate as a switch on UNI-DCE interfaces, NNI interfaces, or a combination of the two. NNI is not required. For switched connections, disable routing parameters or attributes.

Note: Make sure that the Enabled parameter is set to Yes in the Answer-Defaults FR-Answer subprofile.

Settings in a Connection profile

Following are the relevant circuit parameters, shown with sample settings:

```
Ethernet
   Connections
      caller-1
```

```
Name=caller-1
Active=Yes
Encaps=FR-Cir
Encaps options
   FR Prof=max
   DLCI=100
   FR Circuit=frcir1
```

Parameter	Specifies
Encaps	Encapsulation protocol. Both end points of the circuit must specify Frame Relay-Circuit encapsulation.
FR Prof	Name of the Frame Relay profile that defines the datalink.
DLCI	A DLCI for this PVC end point.Obtain the DLCI from your Frame Relay provider. The DSL Terminator does not allow you to enter duplicate DLCIs, except when they are carried by separate physical links specified in different Frame Relay profiles.
FR Circuit	Circuit name (up to 16 characters). The other end point must specify the same circuit name. If only one profile specifies a circuit name, data received on the specified DLCI is dropped. If more than two profiles specify the same circuit name, only two of the profiles are used to form a circuit.

Settings in a RADIUS profile

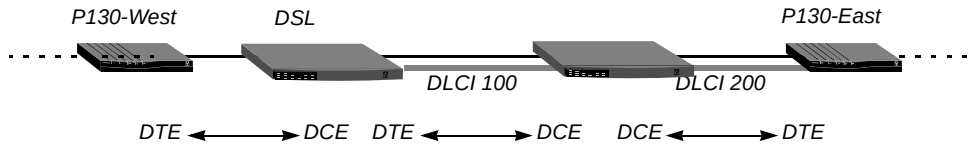
Following are the RADIUS attributes for configuring a Frame Relay circuit:

Attribute	Value
Framed-Protocol (7)	Encapsulation protocol. Both end points of a circuit must specify FR-CIR (263) encapsulation.
Ascend-FR-Profile-Name (180)	Name of the Frame Relay profile that defines the datalink.
Ascend-FR-DLCI (179)	A DLCI for this PVC end point. Do not enter duplicate DLCIs, except when they are carried by separate physical links specified in different Frame Relay profiles.
Ascend-FR-Circuit-Name (156)	Circuit name (up to 16 characters). The other end point must specify the same circuit name. If only one profile specifies a circuit name, data received on the specified DLCI is dropped. If more than two profiles specify the same circuit name, only two of the profiles are used to form a circuit.

Examples of a circuit between UNI interfaces

Figure 5-8 shows a circuit configuration using UNI-DCE interfaces in the DSL Terminator.

Figure 5-8. Frame Relay circuit with UNI interfaces



Using local profiles

The following parameters on the DSL Terminator define the datalinks to the DSL Terminator and to the Pipeline 130 (P130-East):

```
Ethernet
   Frame Relay
      max
         Name=max
         Active=Yes
         FR Type=DCE
         Nailed Grp=111


Ethernet
   Frame Relay
      p130east
         Name=p130east
         Active=Yes
         FR Type=DCE
         Nailed Grp=222
```

The next set of parameters specifies the circuit between the two Frame Relay interfaces:

```
Ethernet
   Connections
      max6
         Name=max6
         Active=Yes
         Encaps=FR-Cir
         Route IP=No
         Encaps options
            FR Prof=max
            DLCI=100
            FR Circuit=frcir1


Ethernet
   Connections
      p130
         Name=p130
         Active=Yes
         Encaps=FR-Cir
         Encaps options
            FR Prof=p130east
```

```
DLCI=200
FR Circuit=frcir1
```

Using RADIUS profiles

The following RADIUS frdlink pseudo-user profiles define the datalinks to the DSL Terminator and to the Pipeline 130 (P130-East):

```
frdlink-max-21 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "max",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DCE,
    Ascend-FR-Nailed-Grp = 111

frdlink-max-22 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "p130east",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DCE,
    Ascend-FR-Nailed-Grp = 222
```

The next set of profiles specifies the circuit between the two Frame Relay interfaces:

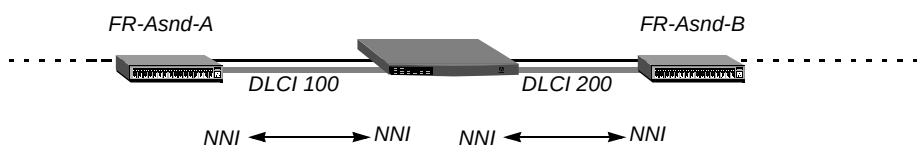
```
permconn-max-10 Password = "ascend", User-Service = Dialout-Framed-
User
    User-Name = "max6",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 100,
    Ascend-FR-Profile-Name = "max",
    Ascend-FR-Circuit-Name = "fr-cir1"

permconn-max-11 Password = "ascend", User-Service = Dialout-Framed-
User
    User-Name = "p130",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 200,
    Ascend-FR-Profile-Name = "p130east",
    Ascend-FR-Circuit-Name = "fr-cir1"
```

Examples of a circuit between NNI interfaces

Figure 5-9 shows a circuit configuration that uses NNI interfaces.

Figure 5-9. Frame Relay circuit with NNI interfaces



Using local profiles

The following parameters on the DSL Terminator define the datalinks to the two switches labeled FR-Asnd-A and FR-Asnd-B:

```
Ethernet
   Frame Relay
      fr-asnd-a
         Name=fr-asnd-a
         Active=Yes
         FR Type=NNI
         Nailed Grp=333

Ethernet
   Frame Relay
      fr-asnd-b
         Name=fr-asnd-b
         Active=Yes
         FR Type=NNI
         Nailed Grp=444
```

The next set of parameters specifies the circuit between the two Frame Relay interfaces:

```
Ethernet
   Connections
      asnd-a
         Name=asnd-a
         Active=Yes
         Encaps=FR-Cir
         Route IP=No
         Encaps options
            FR Prof=fr-asnd-a
            DLCI=100
            FR Circuit=pvc-pipe

Ethernet
   Connections
      asnd-b
         Name=asnd-b
         Active=Yes
         Encaps=FR-Cir
         Route IP=No
         Encaps options
            FR Prof=fr-asnd-b
            DLCI=200
            FR Circuit=pvc-pipe
```

Using RADIUS profiles

The following frdlink pseudo-user profiles define the datalinks to the two switches labeled FR-Asnd-A and FR-Asnd-B:

```
frdlink-max-23 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "fr-asnd-a",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-NNI,
    Ascend-FR-Nailed-Grp = 333
frdlink-max-24 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "fr-asnd-b",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-NNI,
    Ascend-FR-Nailed-Grp = 444
```

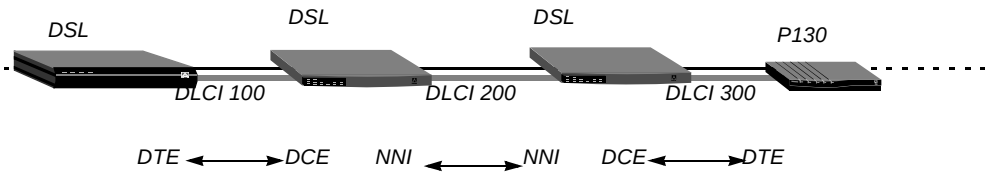
The next set of profiles specifies the circuit between the two Frame Relay interfaces:

```
permconn-max-12 Password = "ascend", User-Service = Dialout-Framed-
User
    User-Name = "asnd-a",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 100,
    Ascend-FR-Profile-Name = "fr-asnd-a",
    Ascend-FR-Circuit-Name = "pvc-pipe"
permconn-max-13 Password = "ascend", User-Service = Dialout-Framed-
User
    User-Name = "asnd-b",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 200,
    Ascend-FR-Profile-Name = "fr-asnd-b",
    Ascend-FR-Circuit-Name = "pvc-pipe"
```

Examples of circuits that use UNI and NNI interfaces

Figure 5-10 shows circuit configurations that use one UNI-DCE and one NNI interface.

Figure 5-10. Frame Relay circuit with UNI and NNI interface



Using local profiles

The following parameters on DSL Terminator-42 define the datalinks to the DSL Terminator-39:

```
Ethernet
   Frame Relay
      dce-max
         Name=dce-max
         Active=Yes
```

```
         FR Type=DCE
         Nailed Grp=555

Ethernet
   Frame Relay
      nni-39
         Name=nni-39
         Active=Yes
         FR Type=NNI
         Nailed Grp=999
```

The next set of parameters on DSL Terminator-42 specifies the circuit between its two Frame Relay interfaces:

```
Ethernet
   Connections
      max
         Name=max
         Active=Yes
         Encaps=FR-Cir
         Route IP=No
         Encaps options
            FR Prof=dce-max
            DLCI=100
            FR Circuit=cir-42

Ethernet
   Connections
      max39
         Name=max39
         Active=Yes
         Encaps=FR-Cir
         Route IP=No
         Encaps options
            FR Prof=nni-39
            DLCI=200
            FR Circuit=cir-42
```

The following parameters on DSL Terminator-39 define the datalinks to DSL Terminator-42 and to the Pipeline 130:

```
Ethernet
   Frame Relay
      nni-42
         Name=nni-42
         Active=Yes
         FR Type=NNI
         Nailed Grp=777

Ethernet
   Frame Relay
```

```
      dce-p130
         Name=dce-p130
         Active=Yes
         FR Type=dce
         Nailed Grp=888
```

The next set of parameters on DSL Terminator-39 specifies the circuit between its two Frame Relay interfaces:

```
Ethernet
   Connections
      max42
         Name=max42
         Active=Yes
         Encaps=FR-Cir
         Route IP=No
         Encaps options
            FR Prof=nni-42
            DLCI=200
            FR Circuit=cir-39

Ethernet
   Connections
      max39
         Name=max39
         Active=Yes
         Encaps=FR-Cir
         Route IP=No
         Encaps options
            FR Prof=dce-p130
            DLCI=300
            FR Circuit=cir-39
```

Using RADIUS profiles

The following profiles define the datalinks from DSL Terminator-42 to the DSL Terminator and DSL Terminator-39:

```
frdlink-max-25 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "dce-max",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DCE,
    Ascend-FR-Nailed-Grp = 555

frdlink-max-26 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "nni-39",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-NNI,
    Ascend-FR-Nailed-Grp = 999
```

The next set of profiles specifies the circuit on DSL Terminator-42:

```
permconn-max-14 Password = "ascend", User-Service = Dialout-Framed-
User
    User-Name = "max"
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 100,
    Ascend-FR-Profile-Name = "dce-max",
    Ascend-FR-Circuit-Name = "cir-42"

permconn-max-15 Password = "ascend", User-Service = Dialout-Framed-
User
    User-Name = "max39",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 200,
    Ascend-FR-Profile-Name = "nni-39",
    Ascend-FR-Circuit-Name = "cir-42"
```

The following profiles define the datalinks from DSL Terminator-39 to DSL Terminator-42 and the Pipeline 130:

```
frdlink-max-27 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "nni-42",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-NNI,
    Ascend-FR-Nailed-Grp = 777

frdlink-max-28 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "dce-p130",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DCE,
    Ascend-FR-Nailed-Grp = 888
```

The next set of profiles specifies the circuit on DSL Terminator-39:

```
permconn-max-16 Password = "ascend", User-Service = Dialout-Framed-
User
    User-Name = "max42"
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 200,
    Ascend-FR-Profile-Name = "nni-42",
    Ascend-FR-Circuit-Name = "cir-39"

permconn-max-17 Password = "ascend", User-Service = Dialout-Framed-
User
    User-Name = "p130",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 300,
    Ascend-FR-Profile-Name = "dce-p130",
    Ascend-FR-Circuit-Name = "cir-39"
```

Frame Relay and ATM internetworking support

FRF.8 Configuration

The DSL Terminator supports Frame Relay Forum Document 8 (FRF.8) internetworking to enable a Frame Relay service user to connect to an ATM service user. The ATM service user performs no frame relaying service-specific functions and the frame relaying service user performs no ATM service-specific functions.

The two operating modes defined for ATM-Frame Relay circuits in the FRF.8 Frame Relay ATM/PVC Service Internetworking Implementation Agreement are as follows:

- Translation mode—the system substitutes ATM Multiprotocol Encapsulation (RFC 1483) for Frame Relay Multiprotocol Encapsulation (RFC 1490) for data traveling from the Frame Relay circuit to the ATM circuit. The opposite process is performed on data traveling from the ATM circuit to the Frame Relay circuit.
- Transparent mode—the system simply passes the data stream from one side of the circuit to the other without any conversion.

Use the default translation mode unless proprietary protocols such as those developed for packetized Voice-over-IP require the use of the transparent mode.

To set up an ATM-Frame Relay circuit, you must properly configure both the ATM and Frame Relay connections. Set the Encaps options in both the ATM and Frame Relay connection profiles with the same circuit name.

For the ATM connection profile, set the Encaps option to ATM-FR_CIR. Following is an example of an ATM connection profile:

```
Ethernet
   Connections

      Station=atm-fr-sw
      Active=Yes
      Encaps=ATM-FR_CIR
      PRI # Type=N/A
      NumPlanID =ISDN
      Dial #=N/A
      Route IP=N/A
      Bridge=N/A
      Dial brdcast=
      Shared Prof=No
      Encaps options...
      Ip options...
      Session options...
      Telco options...
      Accounting...
      DHCP options...

      Encaps options...
         vpi=0
         vci=33
         Circuit=frswitch
         FRF.8 Mode=Translation
```

The FRF.8 parameter is defined as follows:

Attribute	Value
FRF.8 Mode	Mode of operation for the ATM-Frame Relay circuit. Specify Translation or Transparent. To enable this parameter, set the Encaps parameter to `ATM-FR_CIR`.

Following is an example of a Frame Relay connection profile:

```
Ethernet
   Connections
      Station=fr-sw1
      Active=Yes
      Encaps=FR_CIR
      PRI # Type=N/A
      NumPlanID =ISDN
      Dial #=N/A
      Route IP=N/A
      Bridge=N/A
      Dial brdcast=N/A
      Shared Prof=No
      Encaps options...
      Ip options...
      Session options
      Telco options...
      Accounting...
      DHCP options...

      Encaps options...
         FR Prof=frt1-1
         DLCI=87
         Circuit=frswitch
```

Configuring IP Routing

6

Introduction to IP routing and interfaces 6-1
Configuring the local IP network 6-7
Configuring system-level routing policies 6-11
Configuring IP routing connections 6-21
Configuring IP routes and preferences 6-30
Configuring dynamic route updates 6-43

Introduction to IP routing and interfaces

The following tasks are necessary to configure a DSL Terminator for IP routing:

- Setting up the IP network—setting parameters in the DSL Terminator unit's Ethernet profile which set the unit's Ethernet IP interface, network services (such as DNS), and routing policies.
- Configuring IP routing connections—configuring Connection profiles (or similar profiles in an external authentication server) to define destinations across WAN interfaces and to add routes to the routing table.
- Configuring IP routes and preferences and configuring the DSL Terminator for dynamic route updates—configuring the IP profile and individual Connection profiles to set up the IP routing table, which determines the paths over which IP packets are forwarded and specifies the connections to be brought up.

Before you start to configure IP routing on the DSL Terminator, you need to understand the unit's requirements for IP address and subnet format and how the unit uses the routing table, Ethernet interfaces, and WAN interfaces

IP addresses and subnet masks

In a DSL Terminator, you specify IP addresses in dotted decimal format (not hexadecimal). If you specify no subnet mask, the DSL Terminator assumes that the address contains the default

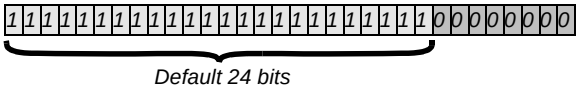
number of network bits for its class. Table 6-1 shows the classes and the default number of network bits for each class (the default subnet mask).

Table 6-1. IP address classes and number of network bits

Class	Address range	Network bits
Class A	0.0.0.0 — 127.255.255.255	8
Class B	128.0.0.0 — 191.255.255.255	16
Class C	192.0.0.0 — 223.255.255.255	24

For example, a class C address, such as 198.5.248.40, has 24 network bits, so its default mask is *24*. The 24 network bits leave 8 bits for the host portion of the address. A single class C network supports up to 253 hosts.

Figure 6-1. Default mask for class C IP address

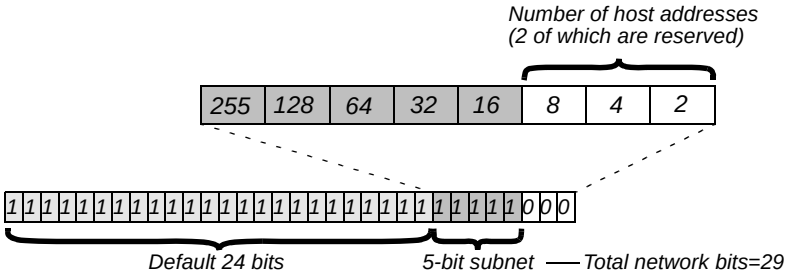


As shown in Figure 6-1, a mask has a binary 1 in each masked position. Therefore, the default, 24-bit, subnet mask for a class C address can be represented in dotted-decimal notation as 255.255.255.0. To specify a different subnet mask, the DSL Terminator recognizes a modifier consisting of a slash followed by a decimal number that represents the number of network bits in the address. For example, 198.5.248.40/29 is equivalent to:

```
IP address = 198.5.248.40
Mask = 255.255.255.248
```

that is, the mask specification indicates that the first 29 bits of the address specify the network. This is a 29-bit subnet. The three remaining bits specify unique hosts, as shown in Figure 6-2.

Figure 6-2. A 29-bit subnet mask and the number of supported hosts



In Figure 6-2, three available bits present eight possible bit combinations. Of the eight possible host addresses, two are reserved, as follows:

000 — Reserved for the network (base address)
001
010
011
100

101
110
111—Reserved for the broadcast address of the subnet

Zero subnets

Early implementations of TCP/IP did not allow zero subnets. Subnets could not have the same base address that a class A, B, or C network would have. For example, while 192.168.8.4/30 was legal, the subnet 192.168.8.0/30 was illegal because it had the same base address as the class C network 192.168.8.0/24. The second example, 192.168.8.0/30, is called a zero subnet, because like a class C base address, its last octet is zero. Modern implementations of TCP/IP enable subnets to have base addresses that can be identical to the class A, B, or C base addresses (Lucent's implementation of RIP 2). You should decide whether or not to support and configure zero subnetworks for your environment. If you configure them in some cases and treat them as unsupported in other cases, you can encounter routing problems.

Table 6-2 shows how the standard subnet address format relates to Lucent's notation for a class C network number.

Table 6-2. Standard subnet masks

Subnet mask	Number of host addresses
255.255.255.128	126 hosts + 1 broadcast, 1 network (base)
255.255.255.192	62 hosts + 1 broadcast, 1 network (base)
255.255.255.224	30 hosts + 1 broadcast, 1 network (base)
255.255.255.240	14 hosts + 1 broadcast, 1 network (base)
255.255.255.248	6 hosts + 1 broadcast, 1 network (base)
255.255.255.252	2 hosts + 1 broadcast, 1 network (base)
255.255.255.254	invalid netmask (no hosts)
255.255.255.255	1 host — a host route

The broadcast address of any subnet has the host portion of the IP address set to all 1s (ones). The network address (or base address) represents the network itself, with the host portion of the IP address set to all zeros. Therefore, these two addresses define the address range of the subnet. For example, if the DSL Terminator configuration assigns the following address to a remote router:

```
IP address = 198.5.248.120
Mask = 255.255.255.248
```

the Ethernet attached to that router has the following address range:

```
198.5.248.120 - 198.5.248.127
```

A host route is a special IP address with a subnet mask of 32 bits. It has a subnet mask of `255.255.255.255` (32 bits).

IP routes

At system startup, the DSL Terminator builds an IP routing table that contains configured routes. When the system is up, it can use routing protocols such as RIP. In each routing table entry, the Destination field specifies a destination network address that can appear in IP packets, and the Gateway field specifies the address of the next-hop router to reach that destination. Each entry also has a preference value and a metric value, which the DSL Terminator evaluates when comparing multiple routes to the same destination.

How the DSL Terminator uses the routing table

The DSL Terminator relies on the routing table to forward IP packets, as follows:

- If the DSL Terminator finds a routing table entry whose Destination field matches a packet's destination address, it routes the packet to the specified next-hop router, whether through its WAN interface or through its Ethernet interface.
- If the DSL Terminator does not find a matching entry, it looks for the Default route, which is identified in the routing table by a destination of 0.0.0.0. If that route has a specified next-hop router, the DSL Terminator forwards the packet to that router.
- If the DSL Terminator does not find a matching entry and does not have a valid Default route, it drops the packet.

Static routes

A static route is a manually configured path from one network to another. It specifies the destination network and the gateway (router) to use to get to that network. If a path to a destination must be reliable, the administrator often configures more than one static route to the destination. In that case, the DSL Terminator chooses the route on the basis of metrics and availability. Each static route has its own Static Rtes profile.

The Ethernet > Mod Config profile specifies a static connected route, which states, in effect, "to reach system X, send packets out this interface to system X." Connected routes are low-cost, because no remote connection is involved.

Each IP-routing Connection profile specifies a static route that states, in effect, "to reach system X, send packets out this interface to system Y," where system Y is another router.

Dynamic routes

A dynamic route is a path to another network that is learned from another IP router (in contrast to a static route which configured in one of the DSL Terminator unit's local profiles). A router that uses RIP broadcasts its entire routing table every 30 seconds, updating other routers about the usability of particular routes. A host that runs ICMP can also send ICMP Redirects to offer a better path to a destination network. Routing protocols, such as RIP, all use some mechanism to propagate routing information and changes through the routing environment.

Route preferences and metrics

Because different protocols have different criteria for assigning route metrics, the DSL Terminator supports route preferences. For example, RIP is a distance-vector protocol, which uses a virtual hop count to select the shortest route to a destination network.

When choosing a route to add to its routing table, the router first compares preference values, preferring the lowest number. If the preference values are equal, the router compares the metric fields and uses the route with the lowest metric. Following are the preference values for the various types of routes:

Route	Default preference
Connected	0
ICMP	30
RIP	100
Static	100
ATMP, PPTP	100

Note: You can configure the DownMetric and DownPreference parameters to assign different metrics and preferences, respectively, to routes on the basis of whether the routes are in use or are down. You can direct the DSL Terminator to use active routes, if available, rather than routes that are down.

DSL Terminator IP interfaces

The DSL Terminator supports routing on Ethernet and WAN interfaces. It can function as either a system-based or interface-based router. Interface-based routing uses numbered IP interfaces.

Ethernet interfaces

The following example shows the routing table for a DSL Terminator configured to enable IP routing:

```
** Ascend DSL Terminator Terminal Server **

ascend% iproute show

Destination        Gateway   IF       Flg   Pref   Met     Use     Age
10.10.0.0/16       -         ie0      C        0     0       3     222
10.10.10.2/32      -         local    CP       0     0       0     222
127.0.0.0/8        -         bh0      CP       0     0       0     222
127.0.0.1/32       -         local    CP       0     0       0     222
127.0.0.2/32       -         rj0      CP       0     0       0     222
224.0.0.0/4        -         mcast    CP       0     0       0     222
224.0.0.1/32       -         local    CP       0     0       0     222
224.0.0.2/32       -         local    CP       0     0       0     222
224.0.0.5/32       -         local    CP       0     0       0     222
224.0.0.6/32       -         local    CP       0     0       0     222
224.0.0.9/32       -         local    CP       0     0       0     222
255.255.255.255/32 -         ie0      CP       0     0       0     222
```

In the preceding example, the Ethernet interface has the IP address 10.10.10.2 (with a subnet mask of 255.255.0.0). No Connection profiles or static routes are configured. At startup, the DSL Terminator creates the following interfaces:

Interface	Description
Ethernet IP	Always active, because it is always connected. You assign its IP address in Ethernet > Mod Config > Ether Options. The DSL Terminator creates two routing table entries: one with a destination of the network (`ie0`), and the other with a destination of the DSL Terminator (`local`).
Black-hole (`bh0`)	Always up. The black-hole address is 127.0.0.0. Packets routed to this interface are discarded silently.
Loopback (`local`)	Always up. The loopback address is 127.0.0.1/32.
Reject (`rj0`)	Always up. The reject address is 127.0.0.2. Packets routed to this interface are sent back to the source address with an ICMP *host unreachable* message.
Not shown in the example	`wanidle0`. Inactive when you configure a Connection profile. Created by the DSL Terminator when WAN connections are down, all routes point to the inactive interface.

WAN IP interfaces

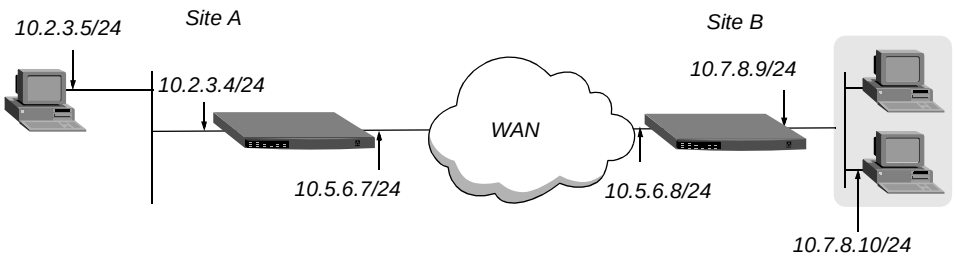
The DSL Terminator creates WAN interfaces as they are brought up. WAN interfaces are labeled wan*N*, where *N* is a number assigned in the order in which the interfaces become active. The WAN IP address can be a local address assigned dynamically when the caller logs in, an address on a subnet of the local network, or a unique IP network address for a remote device.

Numbered interfaces

The DSL Terminator can operate as both a system-based and an interface-based router. Interface-based routing uses numbered interfaces. Some routers or applications require numbered interfaces. Also, some sites use them for troubleshooting leased point-to-point connections and forcing routing decisions between two links going to the same final destination. More generally, interface-based routing enables the DSL Terminator to operate in much the same way as a multihomed Internet host.

Figure 6-3 shows an example of an interface-based routing connection.

Figure 6-3. Interface-based routing example



At Site A, The DSL Terminator assigns IP addresses 10.5.6.7 and 10.5.6.8 to the WAN interfaces. The DSL Terminator route and uses these interface addresses to route packets to the remote network 10.7.8.0.

With system-based routing, the DSL Terminator does not assign interface addresses. It routes packets to the remote network through the WAN interface it created when the connection was brought up.

Interface-based routing requires that, in addition to the system-wide IP configuration, the DSL Terminator and the far end of the link have link-specific IP addresses, for which you specify the following parameters:

- Connections > IP Options > IF Adrs (the link-specific address for the DSL Terminator)
- Connections > IP Options > WAN Alias (the far end link-specific address)

Alternatively, you can omit the remote side's system-based IP address from the Connection profile and use interface-based routing exclusively. This mechanism is appropriate if, for example, the remote system is on a backbone network that can be periodically reconfigured by its administrators, and you want to refer to the remote system only by its mutually agreed-upon interface address. In this case, the following parameters specify the link-specific IP addresses:

- Connections > IP Options > IF Adrs (the near-end numbered interface)
- Connections > IP Options > LAN Adrs (the far-end numbered interface)

Note that if the only known address is the interface address, you must place it in the IP Adrs parameter rather than the WAN Alias parameter. In such a case, the DSL Terminator creates a host route to the interface address (IP Adrs) and a net route to the subnet of the remote interface, and incoming calls must report their IP Addresses as the value of the IP Adrs parameter.

It is also possible, although not recommended, to specify the local numbered interface (Interface Address) and use the far end device's systemwide IP address (IP Adrs). In this case, the remote interface must have an address on the same subnet as the local (numbered) interface.

Note the following differences in operation when the DSL Terminator uses a numbered interface in contrast to unnumbered (system-based) routing:

- An IP packet generated in the DSL Terminator that is sent to a remote address has a source IP address corresponding to a numbered interface, not the systemwide (Ethernet) address.
- The DSL Terminator adds all numbered interfaces to its routing table as host routes.
- The DSL Terminator accepts IP packets addressed to a numbered interface, considering them to be destined for the DSL Terminator itself. (The packet can arrive over any interface and the numbered interface corresponding to the packet's destination address need not be active.)

Configuring the local IP network

The Ethernet profile consists of system-global parameters that affect all IP interfaces in the DSL Terminator. Following are the related parameters (shown with sample settings):

```
Ethernet
   Mod Config
      Ether1 options…
         IP Adrs=10.2.3.1/24
         2nd Adrs=0.0.0.0/0
```

```
   RIP=Off
   RIP2 Use Multicast=No
   Ignore Def Rt=Yes
   Proxy Mode=Off
   Filter=0
 Ether2 options
   IP Adrs=10.2.3.1/24
   2nd Adrs=0.0.0.0/0
   RIP=Off
   RIP2 Use Multicast=No
   Ignore Def Rt=Yes
   Proxy Mode=Off
   Filter=0

WAN options...
   Pool#1 start=100.1.2.3
   Pool#1 count=128
   Pool#1 name=Engineering Dept.
   Pool#2 start=0.0.0.0
   Pool#2 count=0
   Pool#2 name=
   Pool#3 start=10.2.3.4
   Pool#3 count=254
   Pool#3 name=Marketing Dept.
   Pool#4 start=0.0.0.0
   Pool#4 count=0
   Pool#4 name=
   Pool#5 start=0.0.0.0
   Pool#5 count=0
   Pool#5 name=
   Pool#6 start=0.0.0.0
   Pool#6 count=0
   Pool#6 name=
   Pool#7 start=0.0.0.0
   Pool#7 count=0
   Pool#7 name=
   Pool#8 start=0.0.0.0
   Pool#8 count=0
   Pool#8 name=
   Pool#9 start=0.0.0.0
   Pool#9 count=0
   Pool#9 name=
   Pool#A start=0.0.0.0
   Pool#A count=0
   Pool#A name=
   Pool only=No
   Pool Summary=No

Shared Prof=No
Telnet PW=Ascend

BOOTP Relay...
   BOOTP Relay Enable=No
   Server=NA
   Server=NA

DNS...
   Domain Name=abc.com
   Sec Domain Name=
```

```
   Pri DNS=10.65.212.10
   Sec DNS=12.20 7.23.51
   Allow As Client DNS=Yes
   Pri WINS=0.0.0.0
   Sec WINS=0.0.0.0
   List Attempt=No
   List Size=NA
   Client Pri DNS=0.0.0.0
   Client Sec DNS=0.0.0.0
SNTP Server...
   SNTP Enabled=Yes
   Time zone-UTC+0000
   SNTP host#1=0.0.0.0
   SNTP host#2=0.0.0.0
   SNTP host#3=0.0.0.0
UDP Cksum=No
Adv Dialout Routes=Always
```

Understanding IP network parameters

This section provides some background information about the IP network configuration. For detailed information about each parameter, see the *DSL Terminator Reference Guide.*

Ethernet interface IP addresses

You assign an IP address to an Ethernet interface by configuring the IP Adrs parameter in Ethernet>Mod Config>Ether1 options.

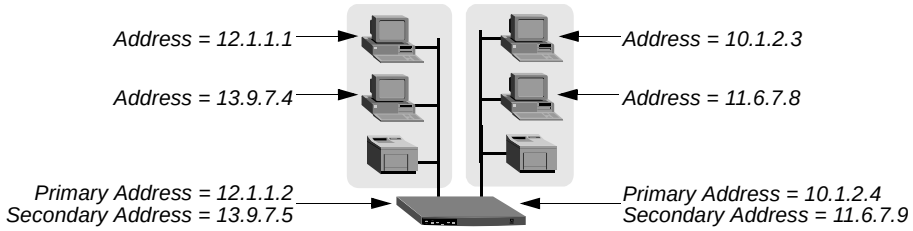
Parameter	Description
IP Adrs	Specifies the DSL Terminator unit's IP address for each local Ethernet interface. To specify the IP addresses for a DSL Terminator Ethernet interface, you must specify the subnet mask. IP address and subnet mask are required settings for the DSL Terminator to operate as an IP router.

The DSL Terminator can assign two unique IP addresses to *each* physical Ethernet port and route between them. This feature, referred to as *dual IP*, can give the DSL Terminator a logical interface on each of two networks or subnets on the same backbone. The advantages of using dual IP include the following:

- A single wire can support two separate IP networks, with devices on the wire assigned to one network or the other and communicating by routing through the DSL Terminator.
- Distribute the routing of traffic to a large subnet by assigning IP addresses on that subnet to two or more routers on the backbone. When a router has a direct connection to the subnet as well as to the backbone network, it routes packets to the subnet and includes the route in its routing table updates.
- An administrator can make a smooth transition when changing IP addresses. A second IP address can act as a placeholder while an administrator make the transition to another network equipment.

Figure 6-4 shows two IP addresses assigned to each of the DSL Terminator unit's Ethernet interfaces.

Figure 6-4. Sample dual IP network



The IP addresses 10.1.2.4 and 11.6.7.9 are assigned to one interface of the DSL Terminator while the IP addresses 1.12.1.1.2 and 13.9.7.5 are assigned to the other interface. In this example, the DSL Terminator routes between all displayed networks. For example, the host assigned with the IP address 12.1.1.1 can communicate with the host assigned 13.9.7.4, the host assigned 10.1.2.3, and the host assigned 11.6.7.8. The host assigned 12.1.1.1 and the host assigned 13.9.7.4 share a physical cable segment, but cannot communicate unless the DSL Terminator routes between the 12.0.0.0 network and the 13.0.0.0 network.

Enabling RIP on the Ethernet interface

You can configure each IP interface to send RIP updates (inform other local routers of its routes), receive RIP updates (learn about networks that can be reached through other routers on the Ethernet), or both.

Note: Lucent recommends that you run RIP version 2 (RIP-v2) if possible. Do not run RIP-v2 and RIP-v1 on the same network in such a way that the routers receive each other's advertisements. RIP-v1 does not propagate subnet mask information and the default-class network mask is assumed, while RIP-v2 handles subnet masks explicitly. Running the two versions on the same network can result in RIP-v1 class subnet mask assumptions overriding accurate subnet information obtained using RIP-v2.

Ignoring the default route

Lucent recommends that you configure the DSL Terminator to ignore default routes advertised by routing protocols. Typically, you do not want the default route changed by a RIP update. The default route specifies a static route to another IP router, which is often a local router. When you configure the DSL Terminator to ignore the default route, RIP updates do not modify the default route in the DSL Terminator routing table.

Proxy ARP and inverse ARP

You can configure the DSL Terminator to respond to an ARP request with its own MAC address. The DSL Terminator also supports Inverse Address Resolution Protocol (Inverse ARP). Inverse ARP enables the DSL Terminator to resolve the protocol address of another device when the hardware address is known. The DSL Terminator does not issue any Inverse ARP requests, but it does respond to Inverse ARP requests that have the protocol type of IP (8000 hexadecimal), or in which the hardware address type is the two-byte Q.922 address (Frame Relay). All other types are discarded. The Inverse ARP response packet sent by the DSL Terminator includes the following information:

- ARP source-protocol address (the DSL Terminator unit's IP address on Ethernet)

- ARP source-hardware address (the Q.922 address of the local DLCI)

(For the details about Inverse ARP, see RFC 1293 and RFC 1490.)

Configuring system-level routing policies

Depending on the requirements of your network environment, you need to configure system-global routing policies in addition to the LAN interface. Services available for the DSL Terminator include:

- Dynamic IP addressing
- Boot Protocol (BOOTP) requests
- Name resolution services: Domain Name System (DNS) and Windows Internet Name Service (WINS)
- Dynamic Host Configuration Protocol (DHCP)
- Network Address Translation (NAT)

Additional system-level services include system time, Telnet password, shared Connection profiles, suppression of dial-out route advertisement in redundant configurations when a trunk fails, UDP checksums, and suppression of host route advertisements.

For detailed information about each parameter in the following sections, see the *DSL Terminator Reference.*

Dynamic IP addressing for dial-in hosts

For dial-in PPP clients not running as IP routers, the DSL Terminator can assign each connection to a local IP address on a first-come, first-served basis. After the connection is terminated, the address that was assigned to that connection is returned to the pool for reassignment to another connection.

Enabling dynamic address assignment

To enable the DSL Terminator for dynamic address assignment, set the Assign Address parameter in the Answer profile to Yes.

Specifying address pools

You can define up to ten address pools in the Ethernet profile, with each pool supporting up to 254 addresses. The Pool#*N* Start parameter specifies the first address in a block of contiguous addresses on the local network or subnet. The Pool#*N* Count parameter specifies how many addresses are in the pool (up to 254). Addresses in a pool do not accept a subnet mask 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, either by statically configuring these routes or configuring the DSL Terminator to dynamically send updates.

Forcing callers configured for a pool address to accept dynamic assignment

During PPP negotiation, a caller can reject the IP address offered by the DSL Terminator and present its own IP address for consideration. Connection profiles compare IP addresses as part of authentication, so the DSL Terminator automatically rejects such a request, if the caller has a Connection profile. However, Name-Password profiles have no such authentication mechanism, and can potentially enable a caller to spoof a local address. The Pool Only parameter can instruct the DSL Terminator to hang up if a caller rejects the dynamic assignment.

Summarizing host routes in routing table advertisements

IP addresses assigned dynamically from a pool are added to the routing table as individual host routes. You can summarize this network (the entire pool), significantly cutting down on route flappage and the size of routing table advertisements.

To enable or disable route summarization (which summarizes a series of host routes into a network route advertisement), set the Pool Summary parameter. The DSL Terminator routes packets destined for a valid host address on the summarized network to the host and rejects packets destined for an invalid host address 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 #*N* Start address must be the first host address. Subtract one from the Pool #*N* Start address to determine the network address (the zero address on the subnet). Because the first and last address of a subnet are reserved, you must set Pool #*N* Count to a value that is two less than a power of two. For example, you can use values 2, 6, 14, 30, 62, 126 or 254. The subnet mask includes a value that is two greater than Pool #*N* Count. For example, with the configuration

```
Pool Summary=Yes
Pool#1 Start=10.12.253.1
Pool#1 Count=126
```

the network alignment address is (Pool Start #1 –1) 10.12.253.0 and the subnet mask is (Pool #1 Count +2 addresses) 255.255.255.128. The resulting address-pool network is:

10.12.253.0/25

For a sample configuration that shows route summarization, see “Configuring DNS” on page 6-17.

Summarizing host routes using RADIUS

Before setting up the pool summary feature in RADIUS, set the Pool Summary parameter to Yes in the Ethernet > Mod Config > WAN Options menu.

To set up the pool summary feature, follow these steps:

1 Using the Ascend-IP-Pool-Definition attribute, make sure that each and every address pool is network aligned.

For an address pool to be network aligned, these conditions must apply:

– The first address in the pool must be the first host address.

The value `first_ipaddr` 1 determines the network alignment—that is, the zero address on the subnet. `first_ipaddr` specifies the first IP address in the pool for the Ascend-IP-Pool-Definition attribute.

– The maximum number of entries you specify with the `max_entries` argument of Ascend-IP-Pool-Definition must be two less than the total number of addresses in the pool.

The value `max_entries` + 2 determines the total number of addresses in the subnet. You can calculate the subnet mask based on this total.

For example, suppose you have this specification for Ascend-IP-Pool-Definition:

```
Ascend-IP-Pool-Definition="1 10.12.253.1 62"
```

Because `first_ipaddr`=10.12.253.1, the network alignment address is 10.12.153.0 (`first_ipaddr` – 1).

Because `max_entries`=62, specify a subnet mask for 64 addresses (`max_entries` + 2). The subnet mask for 64 addresses is 255.255.255.192. (Note that 256–64=192). The Lucent notation for a 255.255.255.192 subnet mask is /26.

The resulting address pool network is 10.12.253.0/26. This address and subnet mask become the first values you specify for the Framed-Route attribute in step 2.

2 Create the first line of a pseudo-user profile containing static routes using the User-Name, Password, and User-Service attributes.

You can configure pseudo-users for both global and unit-specific configuration control of IP routes. The DSL Terminator adds the unit-specific routes in addition to the global routes.

For a unit-specific IP route, specify the first line of a pseudo-user profile in this format:

```
Route-unit_name-num Password="Ascend", User-Service=
Dialout-Framed-User
```

For a global IP route, specify the first line of a pseudo-user profile in this format:

```
Route-num Password="Ascend", User-Service=Dialout-Framed-
User
```

where `unit_name` is the system name of the DSL Terminator—that is, the name specified by the name parameter in the System profile. *`num`* is a number in a sequential series, starting at 1.

For each Framed-Route attribute, specify the host address and subnet mask for a summarized address pool.

The Framed-Route attribute has this format:

```
Framed-Route="host_ipaddr[/subnet_mask] router_ipaddr
metric [private] [profile_name][preference]"
```

For the `host_ipaddr` argument, specify the address of the summarized network. For the `subnet_mask` argument, specify the associated subnet mask.

3 For the `router_ipaddr` argument, specify the router address for each summarized network.

Because the DSL Terminator creates a host route for every address assigned from the pools, and because host routes override subnet routes, the DSL Terminator routes packets whose destination matches an assigned IP address from the pool. However, because the DSL Terminator advertises the entire pool as a route, and only privately knows which IP addresses in the pool are active, a remote network might improperly send the DSL Terminator a packet to an inactive IP address.

The router address handles all IP addresses not assigned to users. When the DSL Terminator receives a packet whose IP address matches an unused IP address in a pool, it either returns the packet to the sender with an ICMP reject message, or simply discards the packet.

To enable the router to handle packets with destinations to invalid hosts on the summarized network, you must specify one of these internal interfaces as the `router_ipaddr` argument.

– The reject interface (rj0)

  The reject interface has an IP address of 127.0.0.2. When you specify this address as the router to the destination pool network, the DSL Terminator rejects packets to an invalid host on that network, appending an ICMP host unreachable message.

– The black-hole interface (bh0)

  The black-hole interface has an IP address of 127.0.0.3. When you specify this address as the router to the destination pool network, the DSL Terminator silently discards packets to an invalid host on that network.

4 Set the `metric` argument to 0.

5 Set the `private` argument to `n` for No.

6 Set the `profile_name` argument to the name of the pseudo-user profile.

7 If you want to specify a preference other than the default value of 120, set the `preference`.

For example, to set up a static route for address pool network 10.12.253.0/26 with a reject interface, enter this setting in a pseudo-user profile called Summary:

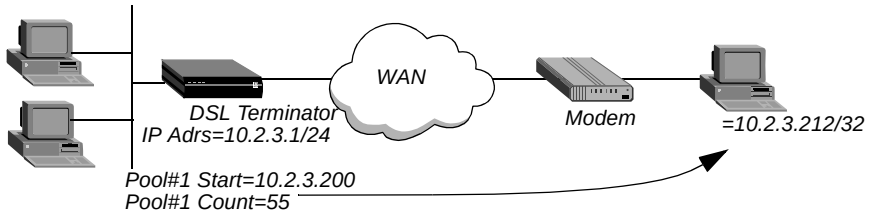
```
Framed-Route="10.12.253.0/26 127.0.0
```

Example of how to set up address pools with route summarization

This example shows how to set up network-aligned address pools and use route summarization. It also shows how to enter a static route for the pool subnet and make the Connection profile route private, both of which are requirements when using route summarization.

The address pool parameters enable the DSL Terminator to assign an IP address to incoming calls that are configured for dynamic assignment. These addresses are assigned on a first-come, first-served basis. After the unit terminates a connection, its address is freed up and returned to the pool for reassignment to another connection. Figure 6-5 shows a host using PPP dial-in software to connect to the unit.

Figure 6-5. Address assigned dynamically from a pool



This example shows how to set up network-aligned address pools and use route summarization.

Following are the rules for network-aligned address pools:

- The Pool#*N* Start address must be the first host address.

  Subtract one from the Pool#*N* Start address for the base address for the subnet.

- The Pool#*N* Count value must be two less than the total number of addresses in the pool.

  Add two to Pool#*N* Count for the total number of addresses in the subnet, and calculate the mask for the subnet on the basis of this total.

For example, the following configuration is network aligned:

```
Ethernet
   Mod Config
      WAN options...
         Pool#1 start=10.12.253.1
         Pool#1 count=62
         Pool#1 name=Engineering Dept.
         Pool Summary=Yes
```

Pool#1 Start is set to 10.12.253.1. When you subtract one from this address, you get 10.12.253.0, which is a valid base address for a subnet defined by a mask of 255.255.255.192. Note that 10.12.253.64, 10.12.253.128, and 10.12.253.192 are also valid zero addresses for the same mask. The resulting address pool subnet is 10.12.253.0/26.

Pool#1 Count is set to 62. When you add two to the value of Pool#1 Count, you get 64. The subnet mask for 64 addresses is 255.255.255.192 (256–64=192). The subnet notation for a 255.255.255.192 mask is /26.

After verifying that *every one* of the configured address pools is network-aligned, you must enter a static route for each of them. These static routes handle all IP address that have not been given to users, by routing them to the reject interface or the black-hole interface (which are defined in “DSL Terminator IP interfaces” on page 6-5).

Note: The DSL Terminator creates a host route for every address assigned from the pools, and host routes override subnet routes. Therefore, packets whose destination matches an assigned IP address from the pool are properly routed and not discarded or bounced. Because the advertises the entire pool as a route, and only privately knows which IP addresses in the pool are active, a remote network can improperly send the DSL Terminator a packet for an inactive IP address. Depending on the static-route specification, these packets are either bounced with an ICMP *host unreachable* message or silently discarded.

For example, the following static route specifies the black-hole interface, so it silently discards all packets whose destination falls in the pool’s subnet. In addition to the Dest and Gateway parameters that define the pool, be sure you have set the Metric, Preference, Cost, and Private parameters as shown.

```
Ethernet
   Static Rtes
      pool-net
         Name=pool-net
         Active=Yes
         Dest=10.12.253.0/26
         Gateway=127.0.0.0
```

```
        Preference=0
        Metric=0
        Cost=0
        Private=No
```

The routing table contains the following lines:

```
Destination         Gateway    IF      Flg       Pref   Met     Use    Age

10.12.253.0/26       -          bh0     C          0      0       0   172162
127.0.0.0/32         -          bh0     CP         0      0       0   172163
127.0.0.1/32         -          lo0     CP         0      0       0   172163
127.0.0.2/32         -          rj0     CP         0      0       0   172163
```

When you configure Connection profiles to assign IP addresses from the pool, make sure you set the Private parameter to Yes. For example:

```
Ethernet
   Connections
      Connection profile
         Ip options...
            LAN Adrs=0.0.0.0/0
            WAN Alias=0.0.0.0
            IF Adrs=0.0.0.0/0
            Preference=100
            Cost=0
            Private=Yes
            RIP=Off
            Pool=1
```

Boot Protocol (BOOTP) requests to other networks

By default, the DSL Terminator does not relay Boot Protocol (BOOTP) requests to other networks. You can enable it to do so by setting parameters in the Ethernet > Mod Config > BOOTP Relay profile.

To configure the DSL Terminator to enable BOOTP relay, you must set the Boot Relay Enable parameter to Yes. In addition, you must disable Ethernet > Mod Config > TServ Options >SLIP BOOTP. SLIP BOOTP makes it possible for a computer connecting to the unit over a SLIP connection to use BOOTP. A DSL Terminator supports BOOTP on only one connection. If you enable both SLIP BOOTP and BOOTP relay, you receive an error message.

You can specify the IP address of one or two BOOTP servers with the Server parameters.

If you specify two BOOTP servers, the unit that relays the BOOTP request determines when to use each server. The order of the BOOTP servers in the BOOTP Relay profile does not necessarily determine which server the unit tries first.

Name resolution service (DNS or WINS)

A DSL Terminator uses Domain Name System (DNS) or Windows Internet Name Service (WINS) for translating host names into IP addresses. When the unit is configured for DNS or WINS name resolution, Telnet and Rlogin users can specify hostnames instead of IP addresses.

The following parameters, located in the Ethernet > Mod Config > DNS profile, are used to configure the DSL Terminator for DNS or WINS

Parameter	Description
Shared Prof	Specifies whether the DSL Terminator allows more than one incoming call to share the same Connection profile. This feature relates to IP routing because the sharing of profiles must result in two IP addresses reached through the same profile. In low-security situations, more than one user can share a name and password for accessing the local network. This situation requires sharing a single Connection profile that specifies bridging only or dynamic IP address assignment. Each call would be a separate connection. The name and password would be shared, and a separate IP address would be assigned dynamically to each caller. If a shared profile uses an IP address, it must be assigned dynamically because multiple hosts cannot share a single IP address.
Telnet password	Password required from all users attempting to access the DSL Terminator by Telnet. If, after three attempts a user is unable to enter the correct password, the connection attempt fails.
BOOTP Relay	Enables the DSL Terminator to relay BOOT Protocol (BOOTP) requests to other networks. When this parameter is set to Yes, you must disable SLIP BOOTP in Ethernet > Mod Config > TServ Options. By default, the BOOTP Relay parameter is set to No. SLIP BOOTP enables a computer connecting to the DSL Terminator over a SLIP connection to use the BOOTP. A DSL Terminator supports BOOTP on only one connection. If you enable both SLIP BOOTP and BOOTP relay, you receive an error message. You can specify the IP address of one or two BOOTP servers but you are not required to specify a second BOOTP server. If you specify two BOOTP servers, the DSL Terminator that relays the BOOTP request determines when to use each server. The order of the BOOTP servers in the BOOTP Relay menu does not necessarily determine which server the DSL Terminator tries first.
Local domain name	Specifies the local DNS domain name, which is used for DNS lookups. When you give the DSL Terminator a hostname to look up, it tries various combinations, including appending the configured domain name to the host name. The Sec Domain Name parameter specifies an alternate domain that the DSL Terminator can search (after it has searched the domain specified by the Domain Name parameter).
DNS or WINS name servers	Specifies a host name instead of an IP address. When the DSL Terminator learns about a DNS (or a WINS), a Telnet and Rlogin user can specify a host name instead of an IP address. If you configure a primary and secondary name server, the secondary server is accessed only if the primary one is inaccessible.

Parameter	Description
DNS lists	Specifies the corresponding IP addresses for a host name. The DNS can return multiple addresses for a hostname in response to a DNS query, but it does not include information about the availability of those hosts. A user typically attempts to access the first address in the list. If that host is unavailable, the user must try the next host, and so forth. However, if the access attempt occurs automatically as part of immediate services, the physical connection is torn down when the initial connection fails. To avoid tearing down physical links when a host is unavailable, set the List Attempt parameter to Yes. The List Size parameter specifies the maximum number of hosts listed (up to 35).
Client DNS	Specifies the DNS server address that will be presented to WAN connections during IPCP negotiation. Configure this parameter to protect your local DNS information from WAN users. The Client DNS parameter has two levels: a global configuration that applies to all PPP connections (defined in the Ethernet profile), and a connection-specific configuration that applies only to the WAN connection defined in the Connection profile. Use global client addresses only if none are specified in the Connection profile.

SNTP service	Specifies whether the DSL Terminator uses Simple Network Time Protocol (SNTP) as defined in RFC 1305. With this parameter set to Yes, the DSL Terminator uses SNTP to set and maintain its system time by communicating with an SNTP server. You must also configure at least one SNTP address and specify your time zone as an offset from Universal Time Coordinated (UTC). UTC is the same as Greenwich Mean Time (GMT). Specify the offset in hours, using a 24-hour clock. Because some time zones, such as Newfoundland, do not have 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 behind UTC and is represented as follows:
	`UTC -0130`
	
	For San Francisco, which is 8 hours behind UTC, the time would be:
	`UTC -0800`
	
	For Frankfurt, which is 1 hour ahead of UTC, the time would be:
	`UTC +0100`

Host	Specify up to three server addresses. The DSL Terminator polls the configured SNTP server at 50-second intervals. The DSL Terminator sends SNTP requests to the first address. It sends requests to the second only if the first is inaccessible, and to the third only if the second is inaccessible.

Parameter	Description
UDP checksums	Enables or disables the use of UDP checksums on the interface. If data integrity is of the highest concern for your network and having redundant checks is important, set the UDP checksums parameter to Yes to generate a checksum whenever a UDP packet is transmitted. UDP packets are transmitted for queries and responses related to ATMP, SYSLOG, DNS, ECHOSERV, RADIUS, TACACS, RIP, SNTP, and TFTP. Although setting UDP checksums parameter to Yes can cause a slight decrease in performance, in most environments, the decrease is not noticeable.

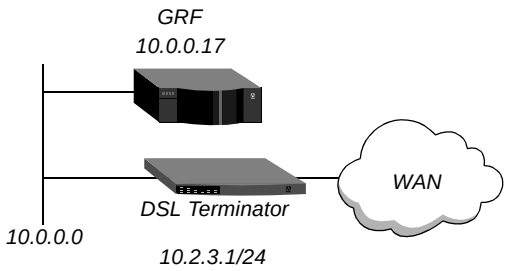
IP network configuration examples

This section shows some examples of Ethernet profile IP configuration. One of the examples, "Configuring DNS" on page 6-17 shows an Ethernet profile, Route profile, and Connection profile configuration that work together.

Configuring the DSL Terminator IP interface on a subnet

On a large corporate backbone, many sites configure subnets to increase the network address space, segment a complex network, and control routing in the local environment. For example, Figure 6-6 shows the main backbone IP network (10.0.0.0) supporting a Lucent GRF router (10.0.0.17).

Figure 6-6. Creating a subnet for the DSL Terminator



You can place the DSL Terminator on a subnet of that network by entering a subnet mask in its IP address specification. For example:

1. Open Ethernet > Mod Config > Ether Options.
2. Specify the IP subnet address for the DSL Terminator on the Ethernet. For example:

```
Ethernet
   Mod Config
      Ether1 options…
         IP Adrs=10.2.3.1/24
```

3. Configure the DSL Terminator to receive RIP updates from the local GRF router:

```
         RIP=Recv=v2
```

4. Close the Ethernet profile.

With this subnet address, the DSL Terminator requires a static route to the backbone router on the main network. Otherwise, it can only communicate with devices on the subnets to which it is directly connected. To create the static route and make the backbone router the default route:

1 Open the Default IP Route profile.

2 Specify the IP address of a backbone router in the Gateway parameter. For example:

```
Ethernet
   Static Rtes
      Name=Default
      Active=Yes
      Dest=0.0.0.0/0
      Gateway=10.0.0.17
      Preference=100
      Metric=1
      DownPreference=140
      DownMetric=7
      Private=Yes
```

3 Close the Default IP Route profile.

For more information about IP Route profiles, see “Configuring IP routes and preferences” on page 6-33. To verify that the DSL Terminator is up on the local network, invoke the terminal-server interface and execute Ping on a local IP address or host name. For example:

```
ascend% ping 10.1.2.3
```

To terminate the Ping exchange, press Ctrl-C.

Configuring DNS

The DNS configuration enables the DSL Terminator to use local DNS or WINS servers for lookups. In the following example of a DNS configuration, client DNS is not in use. You can protect your DNS servers from callers by defining connection-specific (*client*) DNS servers and specifying that Connection profiles use those client servers. To configure the local DNS service:

1 Open Ethernet > Mod Config > DNS.

2 Specify the local domain name.

3 If appropriate, specify a secondary domain name.

4 Specify the IP addresses of a primary and secondary DNS server, and turn on the DNS list attempt feature:

```
Ethernet
   Mod Config
      DNS...
         Domain Name=abc.com
         Sec Domain Name=
         Pri DNS=10.65.212.10
         Sec DNS=12.20 7.23.51
         Allow As Client DNS=Yes
         Pri WINS=0.0.0.0
         Sec WINS=0.0.0.0
         List Attempt=Yes
         List Size=35
         Client Pri DNS=0.0.0.0
```

```
Client Sec DNS=0.0.0.0
```

5 Close the Ethernet profile.

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

You create the DNS table from the terminal server by entering the host names and their IP addresses. A table can contain up to eight entries, with a maximum of 35 IP addresses for each entry. If you specify automatic updating, you only have to enter the first IP address of each host. Any others are added automatically.

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

On the DSL Terminator, the table provides additional information for each table entry. The information is in the following two fields, which the DSL Terminator updates when the system matches the table entry with a hostname not found by the remote server:

- # Reads—Number of reads since the DSL Terminator created the entry. The DSL Terminator updates this field each time it finds a local name query match in the local DNS table.
- Time of Last Read

You can check the list of hostnames and IP addresses in the table by entering the terminal-server command Show DNStab. Figure 6-7 shows an example of a DNS table on a DSL Terminator. Other terminal-server commands show individual entries, with a list of IP addresses for the entry.

Figure 6-7. Local DNS table example

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

Additional terminal-server commands

The terminal-server interface includes Show and DNStab commands have been added to help you view, edit, or and add entries to the DNS table.

Show commands

- `Show ?` displays a list that includes DNStab help.
- `Show dnstab` displays the local DNS table.

- `Show dnstab ?` displays help for the DNStab editor.
- `Show dnstab` entry displays the local DNS table entry (all IP addresses in the list)

DNStab commands

The terminal server DNStab command has the following variations:

DNStab command	Description
DNStab	Displays help information about the DNS table.
DNStab Show	Displays the local DNS table.
DNStab Entry *N*	Displays a list for entry *N* in the local DNS table. The list displayed includes the entry and all the IP addresses stored for that entry up to a maximum number of entries specified in the List Size parameter. If List Attempt=No, no list is displayed.
DNStab Edit	Start editor for the local DNS table.

Configuring the local DNS table

To enable and configure the local DNS table:

1 Display Ethernet > Mod Config > DNS menu.

2 Select a setting for the List Attempt parameter.

3 Specify the list size by setting the List Size parameter.

4 Set the Enable Local DNS Table parameter to Yes. The default is No.

5 Select a setting for the Loc.DNS Tab Auto Update parameter.

Criteria for valid names in the local DNS table

Each name in the local DNS table:
- Must be unique in the table
- Must start with an alphabetic character, which can be either uppercase or lowercase
- Must be less than 256 characters
- Can be a local name or a fully qualified name that includes the domain name

Periods at the ends of names are ignored.

Entering IP addresses in the local DNS table

To enter IP addresses in a local DNS table, use the DNS table editor from the terminal server. While the editor is in use, the system cannot look up addresses in the table or perform automatic updates. A table *entry* is one of the eight table indexes. It includes the hostname, IP address (or addresses), and information fields. To place the initial entries in the table:

1 At the terminal-server interface, type **`dnstab edit`**.

Before you make any entries, the table is empty. The editor initially displays zeros for each of the eight entries in the table. To exit the table editor without making an entry, press Enter.

2 Type an entry number and press Enter.

A warning appears if you type an invalid entry number. If the entry exists, the current name for that entry appears in the prompt.

3 Type the name for the current entry.

If the system accepts the name, it places the name in the table and prompts you for the IP address for the name that you just entered. (For the characteristics of a valid name, see "Criteria for valid names in the local DNS table" on page 6-19.)

If you enter an invalid name, the system prompts you to enter a valid name.

4 Type the IP address for the entry.

If you enter an address in the wrong format, the system prompts you for the correct format. If your format is correct, the system places the address in the table and the editor prompts you for the next entry.

5 When you are finished making entries, type the letter **0** and press Enter when the editor prompts you for another entry.

Editing the local DNS table

To edit the DNS table entries, access the DNS table editor from the terminal server. While the editor is in use, the system cannot look up addresses in the table or perform automatic updates. A table *entry* is one of the eight table indexes. It includes the host name, IP address (or addresses), and information fields. To edit one or more entries in the local DNS table:

1 At the terminal-server interface, type `dnstab edit`

If the table has already been created, the number of the entry last edited appears in the prompt.

2 Type an entry number or press Enter to edit the entry number currently displayed.

A warning appears if you type an invalid entry number. If the entry exists, the current value for that entry appears in the prompt.

3 Replace, accept, or clear the displayed name, as follows:

- To replace the name, type a new name and press Enter.
- To accept the current name, press Enter.
- To clear the name, press the spacebar, then press Enter.

  If you enter a valid name, the system places it in the table (or leaves it there if you accept the current name) and prompts you for the corresponding IP address. (For the characteristics of a valid name, see ""Criteria for valid names in the local DNS table" on page 6-22.)

  If you clear an entry name, all information in all fields for that entry is discarded.

4 Either type a new IP address and press Enter, or leave the current address and just press Enter.

- To change the IP address, type the new IP address.
- To change the name of the entry but not the IP address, just press Enter.

If the address is in the correct format, the system places it in the table and prompts you for another entry.

5 When you are finished making entries, type the letter **0** and press Enter when the editor prompts you for another entry.

Deleting an entry from the local DNS table

To delete an entry from the local DNS table:

1. At the terminal-server interface, type `dnstab edit` to display the table.
2. Type the number of the entry you want to delete and press Enter.
3. Press the spacebar, then press Enter.

Configuring IP routing connections

When you enable IP routing and addresses are specified in a Connection profile, you define an IP WAN interface. Following are the related parameters (shown with sample settings):

```
Ethernet
   Answer
      Assign Adrs=Yes
      PPP options...
         Route IP=Yes

      Session options...
         RIP=Off

Ethernet
   Connections
      Station=remote-device

      Route IP=Yes
      IP options...
         LAN Adrs=0.0.0.0/0
         WAN Alias=0.0.0.0/0
         IF Adrs=0.0.0.0/0
         Preference=100
         Metric=7
         DownPreference=120
         DownMetric=9
         Private=No
         SourceIP Check=No
         RIP=Off
         Pool=0

      Session options...
         IP Direct=0.0.0.0
```

Understanding IP routing connection parameters

This section provides some background information about enabling IP routing in the Answer profile and Connection profiles. For detailed information about each parameter, see the *DSL Terminator Reference Guide.*

Parameter	Description
Assign Adrs	Enables or disables the DSL Terminator to dynamically assign IP address assignment from a pool of designated addresses on the local network. **Note:** You must configure the caller's PPP software to accept an address dynamically. If the Pool Only parameter is set to Yes in the Ethernet profile, the DSL Terminator terminates connections that reject the assigned address during PPP negotiation.
Route IP	Enables or disables the routing of IP data packets on the interface. Set Route IP in Answer > PPP Options to Yes to enable the DSL Terminator to negotiate a routing connection. **Note:** To enable IP packets to be routed for this connection, you must also set the Route IP parameter to Yes in the Connection profile. When you enable IP routing, IP packets are always routed (they are never bridged).

Configuring the remote IP address

The LAN Adrs parameter specifies the IP address of the remote device. Before accepting a call from the far end, the DSL Terminator matches this address to the source IP address presented by the calling device. It can be one of the following values:

Value	How to specify
IP address of a router	If the remote device is an IP router, specify its address, including its subnet mask identifier. (For background information, see "IP addresses and subnet masks" on page 6-1.) If you omit the mask, the DSL Terminator inserts a default subnet mask that makes the entire far-end network accessible.
IP address of a host	If the remote device is running PPP software, specify its address, including a subnet mask identifier of /32 (for example, 10.2.3.4/32).
The null address (0.0.0.0)	If the remote device accepts dynamic address assignment, leave the LANS Adrs parameter blank.

Note: The most common cause of trouble in initially establishing an IP connection is incorrect configuration of the IP address or subnet specification for the remote host or calling device.

Parameter	Description
WAN Alias	Specifies the IP address of the link's remote interface for the WAN, used for numbered-interface routing. The WAN alias is listed in the routing table as a gateway (next hop) to the Lan Adrs value. The caller must use a numbered interface, and its interface address must agree with the WAN Alias setting.
IF Adrs	Specifies another local IP-interface address, to be used as the local numbered interface instead of Ethernet IP Adrs (the default).

Assigning metrics and preferences

Connection profiles often represent switched connections, which have an initial cost that you avoided if you use a nailed-up link to the same destination. To favor nailed-up links, you can assign a higher metric to switched connections than to any of the nailed-up links to the same destination.

Each connection represents a static route, which has a default preference of 100. (For other preferences, see "Route preferences and metrics" on page 6-4.) For each connection, you can fine-tune the route preference or assign a completely different preference.

Note: You can configure the DownMetric and DownPreference parameters to assign different metrics or preferences to routes on the basis of whether the route is in use or is down. You can direct the DSL Terminator to use active routes, if available, rather than choose routes that are down.

Parameter	Description
Private	Specifies whether the DSL Terminator discloses the existence of the route when queried by RIP or another routing protocol. The DSL Terminator uses private routes internally. They are not advertised.
Pool	Specifies an IP-address pool from which the DSL Terminator assigns the caller an IP address. If the Pool parameter is null but all other configuration settings enable dynamic assignment, the DSL Terminator gets IP addresses from the first defined address pool.
IP Direct	Specifies the IP address of a local host that all inbound IP packets on the link will be directed, (bypassing routing and bridging tables for all incoming packets) and sends each packet received to the specified IP address. All outgoing packets are treated as normal IP traffic. They are not affected by the IP Direct configuration. Typically, you configure IP Direct connections with RIP turned off. If you set the IP Direct configuration with RIP set to receive, the DSL Terminator forwards all RIP updates to the specified address. Such a situation is not desirable because RIP updates are designed to be stored locally by the IP router (in this case, the DSL Terminator).

Parameter	Description
Private	Specifies whether the DSL Terminator discloses the existence of the route when queried by RIP or another routing protocol. The DSL Terminator uses private routes internally. They are not advertised.
RIP	Specifies whether an IP interface sends, receives or both updates and receives RIP updates. Lucent recommends that you run RIP version 2 (RIP-v2) if possible. Lucent does not recommend running RIP-v2 and RIP-v1 on the same network in such a way that the routers receive each other's advertisements. RIP-v1 does not propagate subnet mask information, and the default class network mask is assumed, while RIP-v2 handles subnet masks explicitly. Running the two versions on the same network can result in RIP-v1 *guesses* overriding accurate subnet information obtained via RIP-v2.

Checking remote host requirements

IP hosts, such as UNIX systems, Windows or OS/2 PCs, or Macintosh systems, must have appropriately configured TCP/IP software. A remote host calling into the local IP network must also have PPP software.

UNIX software

UNIX systems typically include a TCP/IP stack, DNS software, and other software, files, and utilities used for Internet communication. UNIX network administration documentation describes how to configure these programs and files.

Window or OS/2 software

PCs running Windows or OS/2 need TCP/IP networking software. The software is included with Windows 95, but the user might need to purchase and install it separately if the computer has an earlier version of Windows, or OS/2.

Macintosh software

Macintosh computers need MacTCP or Open Transport software for TCP/IP connectivity. Apple system software versions 7.1 or later include MacTCP. To see if a Macintosh has the software, the user should open the Control Panels folder and look for MacTCP or MacTCP Admin.

Software configuration

For any platform, the TCP/IP software must be configured with the host's IP address and subnet mask. If the host obtains its IP address dynamically from the DSL Terminator, the TCP/IP software must be configured to enable dynamic allocation. If your local network supports a DNS server, you should also configure the host software with the DNS server's address.

Typically, the host software is configured with the DSL Terminator as its default router.

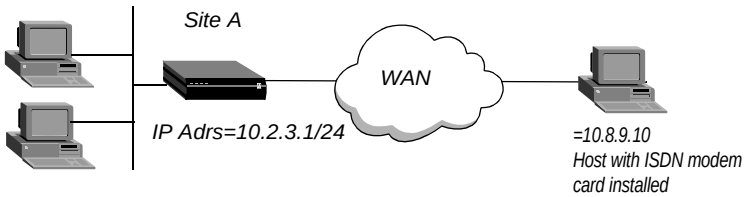
Examples of IP routing connections

This section provides sample Connection profile configurations for IP routing. The examples presume that you have configured the Ethernet profile correctly, as described in "Configuring the local IP network" on page 6-7.

Configuring a host connection with a static address

A host connection with a static address enables the host to keep its own IP address when logging into the DSL Terminator IP network. For example, if a PC user telecommutes to one IP network and uses an ISP on another IP network, one of the connections can assign an IP address dynamically and the other can configure a host route to the PC. This example shows how to configure a host connection with a static address. For details about the /32 subnet mask, see "IP addresses and subnet masks" on page 6-1.)

Figure 6-8. A user requiring a static IP address (a host route)



In this example, the PC at Site B is running PPP software that includes settings like these:

```
Username=patti
Accept Assigned IP=NA (or No)
IP address=10.8.9.10
Subnet mask=255.255.255.255
Default Gateway=NA (or None)
Name Server=10.7.7.1
Domain suffix=abc.com
VAN Jacobsen compression=ON
```

To configure the DSL Terminator to accept dial-in connections from Site B:

1 Open the Answer profile and enable IP routing:

```
Ethernet
   Answer
      PPP options…
         Route IP=Yes
```

2 Close the Answer profile.

3 Open a Connection profile for the dial-in user.

4 Specify the user's name, activate the profile, and set encapsulation options. For example:

```
Ethernet
   Connections
      Station=patti
      Active=Yes
      Encaps=PPP
      Encaps options...
         Send Auth=CHAP
          Recv PW=*SECURE*
```

5 Configure IP routing:

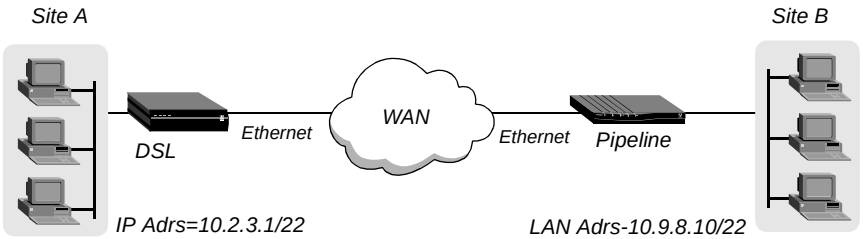
```
Route IP=Yes
IP options…
   LAN Adrs=10.8.9.10/32
   RIP=Off
```

6 Close the Connection profile.

Configuring a router-to-router connection

In this example, the DSL Terminator connects to a corporate IP network and needs a switched connection to another company that has its own IP configuration. Figure 6-9 shows the network diagram.

Figure 6-9. A router-to-router IP connection



This example assumes that the Answer profile in each of the two devices enable IP routing. To configure the Site A DSL Terminator for a connection to Site B:

1 Open a Connection profile for the Site B device.

2 Specify the remote device's name, activate the profile, and set encapsulation options. For example:

```
Ethernet
   Connections
      Station=PipelineB
      Active=Yes
      Encaps=MPP
      Encaps options...
         Send Auth=CHAP
         Recv PW=localpw
         Send PW=remotepw
```

3 Configure IP routing:

```
Route IP=Yes
IP options…
   LAN Adrs=10.9.8.10/22
   RIP=Off
```

4 Close the Connection profile.

To configure the Site B Pipeline:

5 Open the Connection profile for the Site A DSL Terminator.

6 Specify the Site A DSL Terminator unit's name, activate the profile, and set encapsulation options. For example:

```
Ethernet
   Connections
      Station=MAXA
      Active=Yes
      Encaps=MPP
      Encaps options...
         Send Auth=CHAP
         Recv PW=localpw
         Send PW=remotepw
```

7 Configure IP routing.

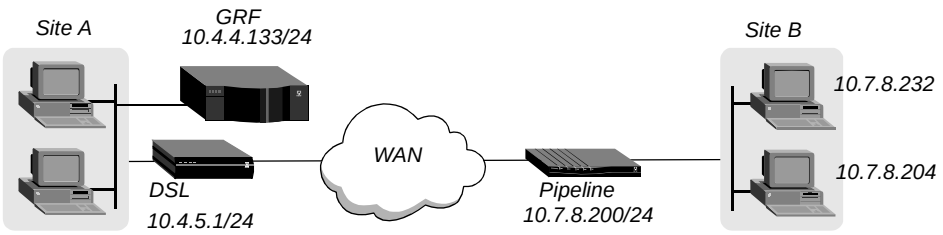
```
Route IP=Yes
IP options…
   LAN Adrs=10.2.3.1/22
   RIP=Off
```

8 Close the Connection profile.

Configuring a router-to-router connection on a subnet

In the sample network shown in Figure 6-10, the DSL Terminator connects telecommuters with their own Ethernet networks to the corporate backbone. The DSL Terminator is on a subnet, and assigns subnet addresses to the telecommuters' networks.

Figure 6-10. A connection between local and remote subnets



This example assumes that the Answer profile in each of the two devices enables IP routing. Because the DSL Terminator specifies a subnet mask as part of its own IP address, the DSL Terminator must use other routers to reach IP addresses outside that subnet. To forward packets to other parts of the corporate network, the DSL Terminator must have either a default route configuration to a router in its own subnet (for example the Cisco router in Figure 5-12) or must enable RIP on Ethernet.

To configure the DSL Terminator at Site A with an IP routing connection to Site B:

1 Open a Connection profile for the Site B device.

2 Specify the remote device's name, activate the profile, and set encapsulation options. For example:

```
Ethernet
   Connections
      Station=PipelineB
      Active=Yes
      Encaps=MPP
      Encaps options...
         Send Auth=CHAP
         Recv PW=localpw
         Send PW=remotepw
```

3 Configure IP routing:

```
Route IP=Yes
IP options…
   LAN Adrs=10.7.8.200/24
   RIP=Off
```

4 Close the Connection profile.

To specify the local Cisco router as the DSL Terminator unit's default route:

1 Open the Default IP Route profile.

2 Specify the Cisco router's address as the gateway address.

```
Ethernet
   Static Rtes
      Name=Default
      Active=Yes
      Dest=0.0.0/0
      Gateway=10.4.4.133
      Metric=1
      Preference=10
      Private=Yes
```

3 Close the IP Route profile.

To configure the Site B Pipeline unit for a connection to Site A:

4 Open the Connection profile in the Pipeline unit for the Site A DSL Terminator.

5 Specify the Site A DSL Terminator unit's name, activate the profile, and set encapsulation options. For example:

```
Ethernet
   Connections
      Station=MAXA
      Active=Yes
      Encaps=MPP
      Encaps options...
         Send Auth=CHAP
         Recv PW=localpw
         Send PW=remotepw
```

6 Configure IP routing:

```
Route IP=Yes
IP options…
   LAN Adrs=10.4.5.1/24
   RIP=Off
```

To make the DSL Terminator the default route for the Site B Pipeline unit:

1 Open the Default IP Route profile in the Site B Pipeline.

2 Specify the DSL Terminator at the far end of the WAN connection as the gateway address:

```
Ethernet
   Static Rtes
      Name=Default
      Active=Yes
      Dest=0.0.0/0
      Gateway=10.4.5.1
      Metric=1
```

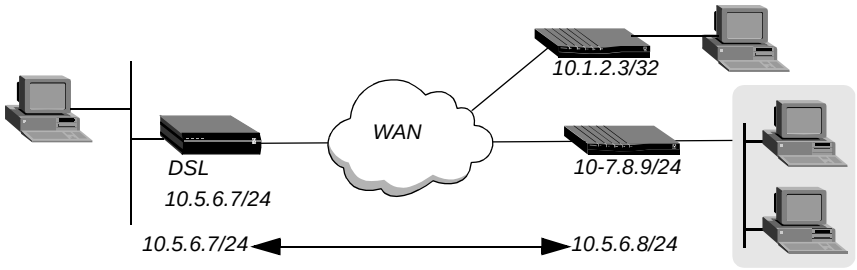
```
      Preference=100
      Private=Yes
```

3 Close the IP Route profile.

Configuring a numbered interface

In the following example, the DSL Terminator is a system-based router but supports a numbered interface for one of its connections. For information about numbered interfaces, see "Numbered interfaces" on page 6-6. The double-headed arrow in Figure 6-11 indicates the numbered interface for this connection.

Figure 6-11. Example of a numbered interface



The numbered interface addresses are:

- IF Adrs—10.5.6.7/24
- WAN Alias—10.5.6.8/24

An unnumbered interface is also shown in Figure 6-10. The 10.1.2.3/32 connection uses a single system-based address for both the DSL Terminator itself and the remote user. To configure the unnumbered interface:

1 Open Ethernet > Mod Config > Ether Options and verify that the IP Adrs parameter is set to the IP address of the Ethernet interface of the DSL Terminator:

```
Ethernet
   Mod Config
      Ether options...
         IP Adrs=10.2.3.4/24
```

2 Close the Ethernet profile.

3 Open the Connection profile and configure the required parameters, then open the IP Options subprofile.

4 Specify the IP address of the Ethernet interface of the remote device by setting the LAN Adrs parameter.

```
Ethernet
      Connections
      IP options...
         LAN Adrs=10.3.4.5/24
```

5 Specify the numbered interface address for the remote device in the WAN Alias parameter.

```
      IP options...
         WAN Alias=10.7.8.9/24
```

6 Close the Connection profile.

Configuring IP routes and preferences

The IP routing table contains routes that are configured (static routes) and routes that are learned dynamically from routing protocols such as RIP. Configuration of static routes involve the following parameters (shown with sample settings):

```
Ethernet
   Static Rtes
      Name=route-name
      Active=Yes
      Dest=10.2.3.0/24
      Gateway=10.2.3.4
      Metric=2
      Preference=100
      Private=No

Ethernet
   Connections
      Route IP=Yes
      IP options...
         LAN Adrs=10.2.3.4/24
         WAN Alias=10.5.6.7/24
         IF Adrs=10.7.8.9/24
         Preference=100
         Metric=7
         DownPreference=120
         DownMetric=9
         Private=No
         SourceIP Check=No
         RIP=Off
         Pool=0
         Multicast Client=No
         Multicast Rate Limit=100
         Multicast Grp Leave Delay=0
         Client Pri DNS=

Ethernet
   Mod Config
      Ether options…
         IP Adrs=10.2.3.1/24
         2nd Adrs=0.0.0.0/0
         RIP=Off
         RIP2 Use Multicast=No
         Ignore Def Rt=Yes
         Proxy Mode=Off
         Filter=0      Route Pref…
         Static Preference=100
         Rip Preference-100
         RIP Queue Depth=
```

Understanding the static route parameters

This section provides some background information about static routes. You can configure static route parameters in Ethernet > Static Routes. For detailed information about each

parameter, see the *DSL Terminator Reference Guide*.

Parameter	Description
2nd Adrs	Assigns a second IP address to the Ethernet interface. With a second address, the DSL Terminator has a logical interface on two networks or two subnets on the same backbone. The configuration is also called *dual IP*. The default value is 0.0.0.0/0.
Active	Enables or disables packet routing. With the Active parameter set to No, the route is ignored.
Client Pri DNS	Specifies a primary DNS server address that the DSL Terminator sends to any IP-routing PPP client connecting to the DSL Terminator. The client DNS feature has two levels: a global configuration that applies to all PPP connections, and a connection-specific configuration that applies to that connection only. The DSL Terminator uses global client addresses only if you specify none in the Connection profile. Also, you can choose to present your local DNS servers if there are no defined or available client servers. You can 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.
Dest	The destination address of a route is the target network (the destination address in a packet). Packets destined for that host use this static route to bring up the right connection. The zero address (0.0.0.0) represents the default route (the destination to which packets are forwarded when there is no route to the packet's destination).
DownMetric	Specifies the metric for a route whose associated WAN connection is down. The higher the metric, the less likely that the DSL Terminator will use the route. You can specify an integer. The default is 7.
DownPreference	Specifies the preference value for a route whose associated WAN connection is down. A higher preference number represents a less desirable route. You can specify an integer. The default is 120.
Filter	Specifies the number of a data filter that applies to the Ethernet interface. You can define the data filter to help manage data flow to and from the Ethernet interface. The filter examines every packet, and forwards or discards the packet on the basis of the configured Filter profile. Specify an integer from 0 to 199. The number you enter depends on the whether you are applying a filter created using the VT100 interface, or a firewall created using Secure Access Manager (SAM).
IF Adrs	Another local IP-interface address, to be used as the local numbered interface instead of the default (the Ethernet IP Adrs).
Gateway	Specifies the IP address of the next-hop router or interface that a packet must go through to reach the route's destination address.

Ignore Def Rt	Specifies whether the DSL Terminator 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 is configured to ignore the default route, RIP updates will not modify the default route in the DSL Terminator routing table. Specify either Yes or No (the default).
IP Adrs	Specifies the DSL Terminator unit's IP address on the local Ethernet. The DSL Terminator creates a route for this address at system startup.
LAN Adrs	Specifies the IP address of Ethernet interface of the remote-end host or router. You can specify a valid IP address and subnet mask.
Metric	Specifies a RIP metric associated with the IP route in a Connection or Route profile. In the Answer profile, it specifies the RIP metric of the IP link when the DSL Terminator validates an incoming call using RADIUS or TACACS and Use Answer as Default is enabled.
Multicast Client	Specifies whether hosts on the other side of the WAN are using IP multicasting. The unit forwards multicast frames to the interface only if a host with the same group has been detected on this interface. The Yes value specifies that hosts on the other side of the WAN are using IP multicasting. The default value, No, specifies that hosts on the other side of the WAN are not using IP multicasting. If multicast forwarding is disabled or if the Connection profile is the Mbone profile (linking to a remote multicast router), this parameter does not apply.
Multicast GRP Leave Delay	Specifies the number of seconds the DSL Terminator waits before forwarding any IGMP version 2, `leave group` message from any multicast client. The default value is 0 (zero). If you specify a value other than the default, and the DSL Terminator receives a `leave group` message, the DSL Terminator sends an IGMP query to the WAN interface from which it received the `leave group` message. If the DSL Terminator does not receive a response from an active multicast client from the same group, it sends a `leave group` message when the time you specified in the Multicast GRP Leave Delay parameter has expired. If you specify the default value of zero, the DSL Terminator forwards any `leave group` message immediately. If users might establish multiple multicast sessions for identical groups, you should set the Multicast GRP Leave Delay parameter to a value from 10 to 20 seconds.
Multicast Rate Limit	Specifies the rate at which the DSL Terminator accepts multicast packets from clients on this interface. It does not affect the MBONE interface. By default, the Rate Limit t parameter is set to 100, *which 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.

Name	To begin forwarding multicast traffic on the interface, set the rate limit to a number less than 100. For example if you set it to 5, the DSL Terminator accepts a packet from multicast clients on the interface every 5 seconds. Any subsequent packets received in that 5-second window are discarded. You can specify a number lower than the default value of 100 to begin forwarding multicast traffic on the interface.
NSSA-ASE7	Specifies that area border routers convert ASE type-7 LSA to an ASE type-5 LSA. ASE type-7s can be imported only from static route definitions. NSSAs are described in RFC 1587. Specify Advertise, or DoNotAdvertise.
Pool	Specifies the IP address pool number that the DSL Terminator assigns to incoming calls. If the Pool parameter is null but all other configuration settings enable dynamic assignment, the DSL Terminator gets IP addresses from the first defined address pool. You can define up to ten IP address pools in the VT100 interface.The default value is 1.
Preference	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.
Private	Specifies whether the DSL Terminator discloses the existence of this route when queried by RIP or another routing protocol. Private routes are used internally but are not advertised. You can specify Yes or No. The default is No.
Proxy Mode	Specifies the conditions under which the DSL Terminator responds to ARP requests for remote devices. With the Proxy Mode parameter enabled, the DSL Terminator responds to the ARP request with its own MAC address. You can specify one of the following values: Off—Disables proxy ARP. This is the default. Always—the DSL Terminator responds to any ARP request with its own MAC address if the ARP request is sent to a host to which the DSL Terminator has a route. Active—the DSL Terminator responds to any ARP request with its own MAC address if the ARP request is sent to a host to which the DSL Terminator has an *active* connection. Inactive—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 an *inactive* connection.
RIP2 Use Multicast	Specifies that Multicast IP is to be used for RIP 2 packets. No is the default.
RIP	Specifies how the DSL Terminator handles RIP update packets on the interface. RIP applies only if the DSL Terminator supports IP routing.You should configure all routers and hosts to 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.You can specify one of the following values:

	Off—the DSL Terminator does not transmit or receive RIP updates. Off is the default. Recv-v2—the DSL Terminator receives RIP-v2 updates on the interface but does not send RIP updates. Send-v2—the DSL Terminator sends RIP-v2 updates on the interface but does not receive RIP updates. Both-v2—the DSL Terminator sends and receives RIP-v2 updates on the interface. Recv-v1—the DSL Terminator receives RIP-v1 updates on the interface but does not send RIP updates. Send-v1—the DSL Terminator sends RIP-v1 updates on the interface but does not receive RIP updates. Both-v1—the DSL Terminator sends and receives RIP-v1 updates on the interface.
RIP Preference	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. You can specify a number from 0 to 255. The default value is 100. Zero (0) is the default for connected routes (such as the Ethernet). The value of 255 means *Do not use this route*.
RIP Queue Depth	Sets the maximum number of unprocessed RIP requests which the DSL Terminator saves. If RIP requests arrive at a rate faster than they can be processed, a backlog builds up. 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. Enter a number from 0 to 1024. If you specify 0, the DSL Terminator saves RIP requests until it runs out of memory. The default is 50.
SourceIP Check	Enables and disables anti-spoofing for this session. With this parameter set to Yes, the system checks all packets received on this interface to ensure that the source IP address in the packets matches the far-end remote address or the address agreed upon in IPCP negotiation. If the addresses do not match, the system discards the packet. You can specify Yes or No. The default value is No.
Static Preference	Specifies the default preference value for statically configured routes. By default, static routes and RIP routes have the same preference, so they compete equally. ICMP redirects take precedence over both. If a dynamic route's preference is lower than that of the static route, the dynamic route can overwrite (*hide)* a static route to the same network. In the IP routing table, the hidden static route has an *h* flag, indicating that it is inactive. The active, dynamically learned route is also in the routing table. However, dynamic routes age and, if no updates are received, eventually expire. In that case, the hidden static route reappears in the routing table.

WAN Alias	Alternate IP address for the remote device, used for numbered-interface routing. The WAN alias will be listed in the routing table as a gateway (next hop) to the Lan Adrs value. The caller must use a numbered interface, and its interface address must agree with the WAN Alias setting.

Examples of static route configuration

This section discusses how to configure the default static route (a static route to a remote subnet) to ensure that the DSL Terminator uses static routes before RIP routes.

For sample Connection profile configurations, see “Configuring IP routing connections” on page 6-24. For an example of the Ethernet profile configuration of the DSL Terminator’s local IP interface, see “Configuring the DSL Terminator IP interface on a subnet” on page 6-19.

Configuring the default route

If no routes exist for the destination address of a packet, the DSL Terminator forwards the packet to the default route. Most sites use the default route to specify a local IP router (such as a Cisco router or a UNIX host running the route daemon) to offload routing tasks to other devices.

Note: If the DSL Terminator does not have a default route, it drops packets for which it has no route.

To configure the default route:

1 Open the first IP Route profile (the route named Default) and activate it:

```
Ethernet
   Static Rtes
      Name=Default
      Active=Yes
      Dest=0.0.0.0/0
```

Note: The name of the first IP Route profile is always Default, and its destination is always 0.0.0.0. You cannot change these values

2 Specify the router to use for packets with unknown destinations. For example:

```
Gateway=10.9.8.10
```

3 Specify a metric for this route, the route’s preference, and whether the route is private. For example:

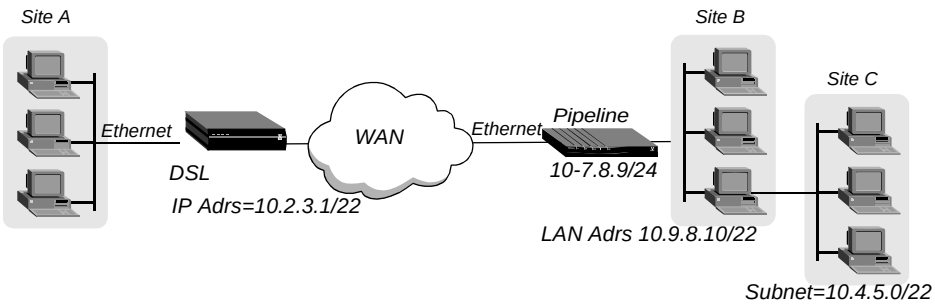
```
Metric=1
Preference=100
Private=Yes
```

4 Close the IP Route profile.

Defining a static route to a remote subnet

If RIP is not enabled on the connection, the DSL Terminator does not learn about other networks or subnets that might be reachable through the remote device. The remote network shown in Figure 6-12 is an example of such a network.

Figure 6-12. Two-hop connection that requires a static route when RIP is off



To enable the DSL Terminator to route to Site C without using RIP, you must configure an IP Route profile similar to the following example:

```
Ethernet
   Static Rtes
      Name=SITEBGW
      Active=Yes
      Dest=10.4.5.0/22
      Gateway=10.9.8.10
      Metric=2
      Preference=100
      Private=Yes
```

Example of route preferences configuration

The following example increases the preference value of RIP routes, instructing the router to use a static route first if one exists:

1 Open Ethernet > Mod Config > Route Pref.

2 Set Rip Preference to 150:

```
Ethernet
   Mod Config
      Route Pref…
         Rip Preference=150
```

3 Close the Ethernet profile.

Configuring static IP routes in RADIUS

In RADIUS, you can create a static route in one of two ways:

- In a pseudo-user profile containing one or more explicit routes
- In a user profile specifying a WAN connection

When the DSL Terminator has a RADIUS user profile that defines a static route to the same destination as one of the DSL Terminator unit's IP Route profiles or a RADIUS pseudo-user profile, the metric in the RADIUS user profile overrides the metric in the other profiles, but only when the RADIUS user connects.

For example, suppose a DSL Terminator has a static route to network 1.10.1.10 with a metric of 10. A user profile in RADIUS has a metric of 7 in a static route to the same network. When

the route is not connected, the DSL Terminator routing table indicates that the route has a metric of 10. When the route is connected, the DSL Terminator routing table indicates that the route has a metric of 7, with an `r` in the flags column to indicate that the route came from RADIUS. Furthermore, the old route with a metric of 10 remains in the routing table, with an asterisk (*) in the flags column, indicating that it is a hidden route.

Specifying static IP routes in a pseudo-user profile

When you disable RIP in a RADIUS user profile (the Framed-Routing parameter is set to None), the DSL Terminator does not listen to RIP updates across that connection. To route to other networks through that connection, the DSL Terminator must rely on static routes you define in a RADIUS pseudo-user profile.

If you configure the DSL Terminator with a subnet address on a backbone network using the IP Adrs parameter in the Ethernet>Mod Config>Ether Options menu, you must set up a static route to the backbone router on the main network. If you do not, the DSL Terminator can only see the subnets to which it directly connects.

You cannot create static routes for dynamically assigned IP addresses, because the actual route to those addresses changes with each dynamic assignment.

To set up static IP routes in a RADIUS pseudo-user profile, proceed as follows:

1 Create the first line of a pseudo-user profile using the User-Name, Password, and User-Service attributes.

You create a pseudo-user profile to store information that the DSL Terminator can query—in this case, in order to store IP routing information. You can configure pseudo-users for both global and DSL Terminator-specific configuration control of IP dialout routes. The DSL Terminator adds the unit-specific dialout routes in addition to the global dialout routes.

For a unit-specific IP dialout route, specify the first line of a pseudo-user profile in this format:

```
Route-unit_name-num Password="Ascend", User-Service=
Dialout-Framed-User
```

For a global IP dialout route, specify the first line of a pseudo-user profile in this format:

```
Route-num Password="Ascend", User-Service=Dialout-Framed-User
```

where `unit_name` is the system name of the DSL Terminator—that is, the name specified by the Name parameter in the System profile. *`num`* is a number in a sequential series, starting at 1.

2 For each pseudo-user profile, specify one or more routes using the Framed-Route attribute.

The Framed-Route attribute has this format:

```
Framed-Route="host_ipaddr[/subnet_mask] router_ipaddr
metric [private] [profile_name][preference]"
```

Limit each profile to about 25 routes—that is, you should specify up to 25 settings for the Framed-Route attribute. The DSL Terminator fetches information from each pseudo-user

profile in order to initialize its routing table. Table 6-3 describes each Framed-Route argument.

Table 6-3. Framed-Route arguments

Syntax element	Description
`host_ipaddr/subnet_mask`	Indicates the IP address of the destination host or subnet reached by the route. The default value is 0.0.0.0/0. If the address includes a subnet mask, the remote router specified by `router_ipaddr` is a router to that subnet, rather than to a whole remote network. To specify the entire remote network, do not specify a subnet mask.
`router_ipaddr`	Specifies the IP address of the router at the remote end of the connection. The default value is 0.0.0.0. The 0.0.0.0 address is a wildcard entry the DSL Terminator replaces with the caller's IP address. When RADIUS authenticates a caller and sends the DSL Terminator an Access-Accept message with a value of 0.0.0.0 for `router_ipaddr`, the DSL Terminator updates its routing tables with the Framed-Route value, but substitutes the caller's IP address for the router. This setting is especially useful when RADIUS cannot know the IP address of the caller because the IP address comes from an address pool.
`metric`	Indicates the metric for the route. If the DSL Terminator has more than one possible route to a destination network, it chooses the one with the lower metric. The default value is 8.
`private`	Specifies `y` if the route is private, or `n` if it is not private. If you specify that the route is private, the DSL Terminator does not disclose the existence of the route when queried by RIP or another routing protocol. The default value is `n`.
`profile_name`	Indicates the name of the outgoing user profile that uses the route. The default value is null.
`preference`	Specifies the preference that the DSL Terminator gives the route.

Whenever you power on or reset the DSL Terminator, or when you select the Upd Rem Cfg command from the Sys Diag menu, RADIUS adds IP dialout routes to the routing table in this way:

1 RADIUS looks for profiles having the format Route-`unit_name`-1, where `unit_name` is the system name.

2 If at least one profile exists, RADIUS loads all existing profiles with the format Route-`unit_name-num` to initialize the IP routing table.

   The variable `num` is a number in a sequential series, starting with 1.

3 The DSL Terminator queries Route-`unit_name`-1, then Route-`unit_name`-2, and so on, until it receives an authentication reject from RADIUS.

4 RADIUS loads the global configuration profiles.

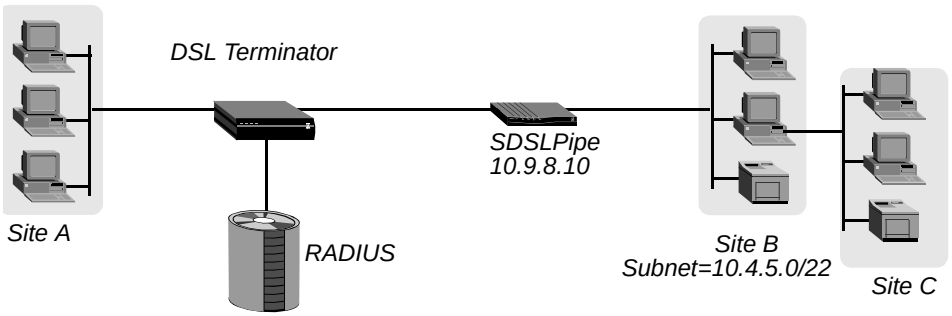
   These configurations have the format Route-`num`.

5 The DSL Terminator queries Route-1, then Route-2, and so on, until it receives an authentication reject from RADIUS.

Static IP route configuration example

The network diagram in Figure 6-13 shows a remote network that does not have its own Connection profile or RADIUS user profile, but can be reached through an existing RADIUS user profile.

Figure 6-13. A two-hop connection that requires a static route when RIP is off



In Figure 6-13, if RIP is disabled in the RADIUS user profile for site B, the DSL Terminator must have a static route like this one to route to site C:

```
Route-1 Password="Ascend", User-Service=Dialout-Framed-User
        Framed-Route="10.4.5.0/22 10.9.8.10 1 n inu-out"
```

Specifying static IP routes in a dial-in user profile

Every Connection profile and RADIUS user profile that specifies an explicit IP address is a static route. For details on creating an implicit static route in a dial-in profile, see the TAOS RADIUS Guide.

In addition, you might wish to update the DSL Terminator unit's routing tables when connecting to a user whose profile specifies User-Service=Framed-User. In this case, you can set the Framed-Route attribute in an incoming user profile to specify the user's IP address and subnet mask with the `host_ipaddr` and `/subnet_mask` arguments. The route you specify in this manner exists only during the time the call is online. However, when you enter a nonzero router address for the `router_ipaddr` argument that is different from the caller's address, the static route of a dial-in framed-user persists even after the connection goes offline.

Configuring dynamic route updates

You can configure each active interface to send or receive RIP. You can also configure the Ethernet interface to accept or ignore ICMP redirects. All of these routing mechanisms modify the IP routing table dynamically.

Following are the parameters (shown with sample values) that enable the DSL Terminator to receive updates from RIP or ICMP.

```
Ethernet
   Mod Config
      Ether options…
         RIP=On
         Ignore Def Rt=Yes
      RIP Policy=Poison Rvrs
      RIP Summary=Yes
      ICMP Redirects=Accept

Ethernet
   Answer
      Session options...
         RIP=On

Ethernet
   Connections
    any Connection profile
      IP options...
         Private=No
         RIP=On
```

Dynamic route configuration

You can configure the DSL Terminator to modify the IP routing table dynamically. To do so, you must configure each active interface to send or receive RIP or OSPF updates. You can also configure the Ethernet interface to accept or ignore ICMP redirects.

The Ethernet > Mod Config > Ether Options profile contains several of the parameters for configuring dynamic route updating:

Parameter	Specifies
RIP	How the DSL Terminator handles RIP updates on the Ethernet interface and on each WAN interface. The RIP parameter in the Ethernet > Answer > Session Options profile applies to local profiles and profiles retrieved from RADIUS. Many sites turn off RIP on WAN connections to keep their routing tables from becoming very large. **Note:** The IETF considers RIP-v1 an historic protocol and its use is no longer recommended. Lucent recommends that you upgrade all routers to RIP-v2. If you must maintain RIP-v1, Lucent recommends that you create a separate subnet for all RIP-v1 routers and hosts.

Ignore Def Rt	Whether the DSL Terminator ignores the default routes advertised by routing protocols. This configuration is recommended, because you typically do not want the default route changed by a RIP update. The default route specifies a static route to another IP router, which is often a local router such as a GRF or another kind of LAN router. When you configure the DSL Terminator to ignore the default route, RIP updates do not modify the default route in the DSL Terminator routing table.
RIP Policy	If the DSL Terminator is running RIP-v1, the RIP Policy parameter 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 being sent. Split-horizon means that the DSL Terminator does not propagate routes back to the subnet from which they were received. Poison-reverse means that it propagates routes back to the subnet from which they were received, but with a metric of 16. This parameter has no affect on RIP-v2.
RIP Summary	Whether the DSL Terminator summarizes subnet information when advertising routes. If the DSL Terminator 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 with a subnet set to 28 bits) is advertised as a route to 200.5.8.0. If the DSL Terminator does not summarize information, it advertises each route in its routing table as is. For the subnet in the preceding example, the DSL Terminator would advertise a route only to 200.5.8.13. This parameter has no affect on RIP-v2.
ICMP Redirects	Enables or disables the DSL Terminator to dynamically find the most efficient IP route to a destination, but they are one of the oldest and least secure route discovery methods on the Internet. ICMP Redirect packets can be counterfeited to change the way a device routes packets. By default, this parameter is set to Ignore. Change the setting to Accept if you want to accept these packets.

If you set the Private parameter to Yes in a Connection profile, the router does not disclose its route in response to queries from routing protocols.

Example of RIP and ICMP configuration

The following sample configuration instructs the DSL Terminator to ignore ICMP Redirect packets, to receive (but not send) RIP updates on the Ethernet interface, and to send (but not receive) RIP updates on a WAN connection.

1 Open Ethernet > Mod Config > Ether Options.

2 Configure the DSL Terminator to receive (but not send) RIP updates on the Ethernet interface:

```
Ethernet
   Mod Config
      Ether options…
         RIP=Recv-v2
```

Receiving RIP updates on the Ethernet interface means that the DSL Terminator learns about networks that are reachable through other local routers. However, it does not propagate information about all of its remote connections to the local routers.

3 Exit the profile and, at the exit prompt, select the `exit and accept` option.

4 Set ICMP Redirects to Ignore:

```
ICMP Redirects=Ignore
```

5 Exit the profile and, at the exit prompt, select the `exit and accept` option.

6 Open the Connection profile in which the link is configured, open the IP Options subprofile, and configure the DSL Terminator to send (but not receive) RIP updates on the link:

```
Ethernet
   Connections
      Connection profile 1
         IP options...
            RIP=Send-v2
```

Sending RIP on a WAN connection enables the remote devices to access networks that are reachable through other local routers. However, the DSL Terminator does not receive information about networks that are reachable through the remote router.

7 Exit the profile and, at the exit prompt, select the `exit and accept` option.

Configuring OSPF Routing

7

OSPF overview 7-1

Configuring OSPF routing in the DSL Terminator 7-8

To configure your DSL Terminator for Open Shortest Path First (OSPF) routing, you need to determine the interfaces—LAN or WAN—on you wish to support the protocol. To configure OSPF for a LAN (Ethernet) interface, you use the Ether Options profile. To configure OSPF for a WAN interface, you use a Connections profile. In addition, you can configure the DSL Terminator unit to add routes from a remote router that does not support OSPF or, in a complex network, configure the DSL Terminator unit as an OSPF internal router.

OSPF overview

OSPF is the next-generation Internet routing protocol designed to overcome the limitations in Routing Information Protocol (RIP) that have occurred as a result of the growth of the Internet.

RIP is a distance-vector protocol, which uses a hop count to select the shortest route to a destination network. RIP always uses the lowest hop count, regardless of the speed or reliability of a link. 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, and whether the link is up or down when determining the best path to a destination network.

With RIP, a destination that requires more than 15 consecutive hops is considered unreachable, which inhibits the maximum size of a network. OSPF has no hop limitation. You can add as many routers to a network as you want.

RIP creates a routing table and then propagates it throughout the internet of routers, hop by hop. With increasing Internet routing traffic, RIP convergence (the time it takes for all routers to receive information about a topology change) is sometimes slow, resulting in routing loops and errors.

A RIP router broadcasts its entire routing table every 30 seconds. On a 15-hop network, convergence can be as high as 7.5 minutes. In addition, a large table can require multiple broadcasts for each update, which consumes a lot of bandwidth. OSPF uses a topological database of the network and propagates only changes to the database, which results in more efficient propagation.

TAOS implementation of OSPF

The primary goal for the TAOS current implementation of OSPF is to enable the DSL Terminator to communicate with other routers within a single Autonomous System (AS). The TAOS implementation includes Area Border Router (ABR) capabilities and MD5 authentication.

The DSL Terminator does not function as a full AS Border Router (ASBR), although it performs ASBR calculations for external routes such as WAN links that do not support OSPF. The DSL Terminator imports external routes into its OSPF database and flags them as Autonomous System External (ASE). It redistributes those routes by means of OSPF ASE advertisements, and propagates its OSPF routes to remote WAN routers that are running RIP.

The DSL Terminator supports null and simple password authentication.

OSPF features

This section provides a brief overview of OSPF routing to help you properly configure the DSL Terminator. For full details about how OSPF works, see RFC 1583, *OSPF Version 2*, 03/23/1994, J. Moy.

An Autonomous System (AS) is a group of OSPF routers exchanging information, typically under the control of one company. An AS can include a large number of networks, all of which are assigned the same AS number. All information exchanged within the AS is *interior.*

Exterior protocols are used to exchange routing information between Autonomous Systems. The protocols are referred to by the acronym EGP (Exterior Gateway Protocol). Border routers can use the AS number to filter out certain EGP routing information. OSPF can make use of EGP data generated by other border routers and added into the OSPF system as ASEs, and can also use static routes configured in the DSL Terminator or RADIUS.

Security

All OSPF protocol exchanges are authenticated. This means that only trusted routers can participate in the AS's routing. A variety of authentication schemes are available. In fact, different authentication types can be configured for each area. In addition, authentication provides added security for the routers that are on the network. Routers that do not have the password cannot gain access to the routing information, because authentication failure prevents a router from forming adjacencies.

OSPF on the DSL Terminator supports the MD5 cryptographic authentication method. You can select the MD5 authentication type to direct the DSL Terminator to validate OSPF packet exchanges using MD5 encryption and an authentication key of as many as 16 characters. The authentication key value in the KeyID field is a number from 0 to 255.

For detailed information about the AuthType and the KeyID parameters, see the *DSL Terminator Reference*.

Support for variable length subnet masks

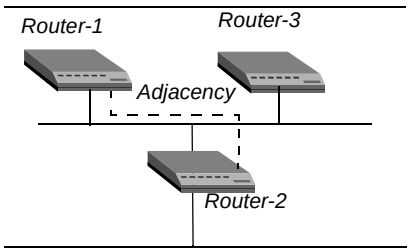
OSPF enables the flexible configuration of IP subnets. Each route distributed by OSPF has a destination and mask. Two different subnets of the same IP network number can have different sizes (different masks). This capability is commonly referred to as Variable Length Subnet Masks (VLSM), or Classless Inter-Domain Routing (CIDR). The DSL Terminator routes a packet to the best (longest, or most specific) match. The DSL Terminator considers host routes to be subnets whose masks are all ones (0xFFFFFFFF).

Note: Although OSPF is very useful for networks that use VLSM, Lucent recommends that you attempt to assign subnets as contiguously as possible, to prevent excessive link-state calculations by all OSPF routers on the network.

Exchange of routing information

OSPF uses a topological database of the network and propagates only changes to the database. Part of the SPF algorithm involves acquiring neighbors and forming an adjacency with one neighbor, as shown in Figure 7-1.

Figure 7-1. Adjacency between neighboring routers



An OSPF router dynamically detects its neighboring routers by sending Hello packets to the multicast address `All SPFRouters`. It then attempts to form adjacencies with some of its newly acquired neighbors.

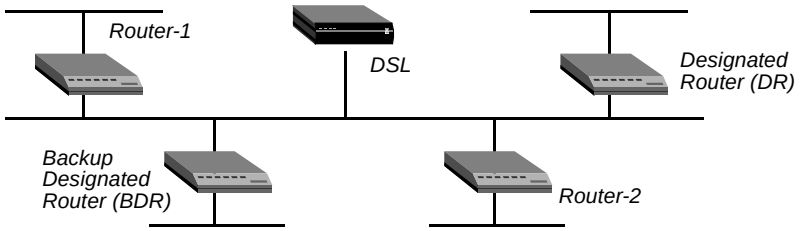
Adjacency is a relationship formed between selected neighboring routers for the purpose of exchanging routing information. Not every pair of neighboring routers becomes adjacent. Adjacencies are established during network initialization in pairs, between two neighbors. As the adjacency is established, the neighbors exchange databases and build a consistent, synchronized database between them.

When an OSPF router detects a change on one of its interfaces, it modifies its topological database and multicasts the change to its adjacent neighbor, which in turn propagates the change to its adjacent neighbor until all routers within an area have synchronized topological databases. The result is quick convergence among routers.

Designated and Backup Designated Routers

In OSPF terminology, a broadcast network is any network that has more than two OSPF routers attached and that supports the capability to address a single physical message to all of the attached routers.

Figure 7-2. Designated and Backup Designated Routers



To reduce the number of adjacencies each router must form, OSPF calls one of the routers the Designated Router. A Designated Router is elected as routers are forming adjacencies, and then all other routers establish adjacencies only with the designated router. This simplifies the routing table update procedure and reduces the number of link-state records in the database. The Designated Router also plays other important roles in reducing the overhead of OSPF link-state procedures. For example, other routers send Link-State Advertisements (LSAs) to only the Designated Router by using the All-Designated-Routers multicast address of 224.0.0.6.

To prevent the Designated Router from becoming a serious liability to the network if it fails, OSPF elects a Backup Designated Router at the same time. Other routers maintain adjacencies with both the Designated Router and its backup router, but the backup router leaves as many of the processing tasks as possible to the Designated Router. If the Designated Router fails, the backup immediately becomes the Designated Router and a new backup is elected.

The administrator chooses which router is to be the Designated Router on the basis of the processing power, speed, and memory of the system, and then assigns priorities to other routers on the network in case the Backup Designated Router is also down at the same time.

Note: The DSL Terminator can function as a Designated Router (DR) or Backup Designated Router (BDR). However, many sites choose to assign a LAN-based router for these roles in order to dedicate the DSL Terminator to WAN processing.

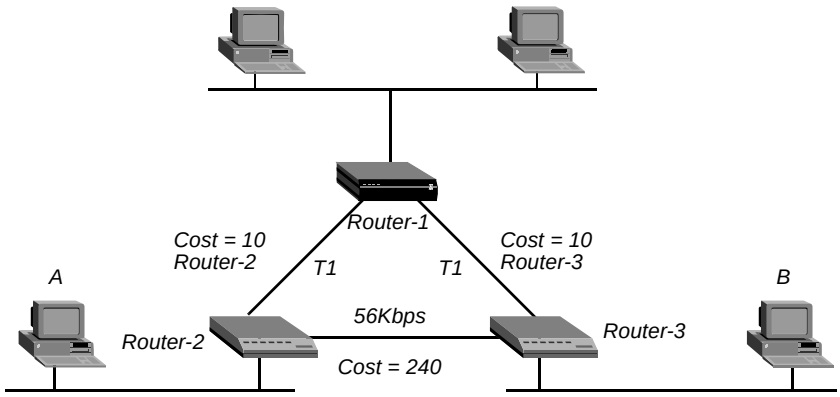
Configurable metrics

The administrator assigns a cost to the output side of each router interface. The lower the cost, the more likely the interface is to be used to forward data traffic. Costs can also be associated with the externally derived routing data.

You can also use the OSPF cost for preferred path selection. If two paths to a destination have equal costs, you can assign a higher cost to one of the paths, to configure it as a backup to be used only when the primary path is not available.

Figure 7-3 shows how costs direct traffic over high-speed links. For example, if Router-2 in Figure 7-3 receives packets destined for Host B, it routes them through Router-1, across two T1 links (Cost=20), rather than across one 56Kbps B-channel to Router-3 (Cost=240).

Figure 7-3. OSPF costs for different types of links



The DSL Terminator has a default cost of one for a connected route (Ethernet) and ten for a WAN link. If you have two paths to the same destination, the DSL Terminator selects the one with the lower cost. You might want to account for the bandwidth of a connection when assigning costs. For example, for a single B-channel connection, the cost would be 24 times greater than for a T1 link.

Note: Be careful when assigning costs. Incorrect cost metrics can cause delays and congestion on the network.

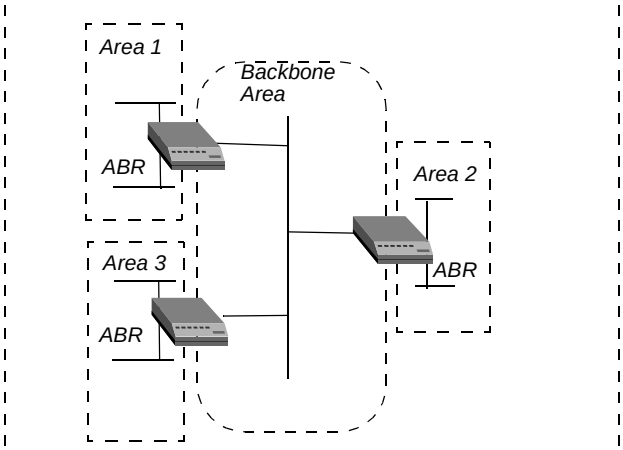
Hierarchical routing (areas)

If a network is large, the size of the database, time required for route computation, and related network traffic can become excessive. An administrator can partition an AS into areas to provide hierarchical routing connected by a backbone.

The backbone area is special and always has the area number 0.0.0.0. Other areas are assigned area numbers that are unique within the Autonomous System.

Each area acts like its own network. All area-specific routing information stays within the area, and all routers within an area must have a synchronized topological database. To tie the areas together, some routers belong to the backbone area and to another area. These routers are Area Border Routers (ABRs). In Figure 7-4, all of the routers are ABRs. If you set up the ABRs and area boundaries correctly, link-state databases are unique to an area.

Figure 7-4. Dividing an AS into areas



Stub areas

For areas that are connected only to the backbone by one ABR (that is, the area has one exit point), there is no need to maintain information about external routes. To reduce the cost of routing, OSPF supports stub areas, in which a default route summarizes all external routes. A stub area allows no Type-5 LSAs to be propagated into or throughout the area, and instead depends on default routing to external destinations.

To prevent flooding of external routes throughout the AS, you can configure an area as a stub if the area has a single exit point or if the choice of exit point need not be made on a per-external-destination basis. You might need to specify a stub area with no default cost (StubNoDefault) if the area has more than one exit point.

In a stub area, routing to AS-external destinations is based on a per-area default cost. The per-area default cost is advertised to all routers within the stub area by a border router, and is used for all external destinations.

Not So Stubby Areas (NSSAs)

The DSL Terminator supports OSPF Not So Stubby Areas (NSSAs) as described in RFC 1587. NSSAs enable you to treat complex networks similarly to stub areas. This can simplify your network's topology and reduce OSPF-related traffic.

NSSAs are similar to stub areas, except that they enable limited importing of AS-external routes. NSSAs use Type-7 LSAs to import external route information into an NSSA. Type-7 LSAs are similar to Type-5 LSAs except that:

- NSSAs can originate and import Type-7 LSAs. Like stub areas, NSSAs cannot originate or import Type-5 LSAs.
- Type-7 LSAs can only be advertised within a single NSSA. They are not flooded throughout the AS as are Type-5 LSAs.

When you configure the DSL Terminator as an NSSA internal router, you define the Type-7 LSAs you want to advertise throughout the NSSA as static routes.

You must also specify whether these Type-7 LSAs should be advertised outside the NSSA. If you choose to advertise a Type-7 LSA, the NSSA Area Border Router (ABR) converts it to a Type-5 LSA, which can then be flooded throughout the AS. If you choose not to advertise a Type-7 LSA, it is not advertised beyond the NSSA.

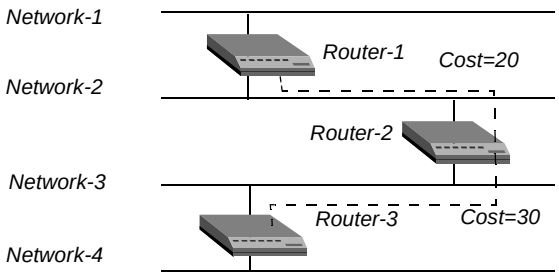
(For complete information about NSSAs, see RFC 1587.)

The link-state routing algorithm

Link-state routing algorithms require that all routers within a domain maintain synchronized (identical) topological databases, and that the databases describe the complete topology of the domain. An OSPF router's domain can be an AS or an area within an AS.

OSPF routers exchange routing information and build link-state databases. Link-state databases are synchronized between pairs of adjacent routers (as described in "Exchange of routing information" on page 7-3). In addition, each OSPF router uses its link-state database to calculate a self-rooted tree of shortest paths to all destinations, as shown in Figure 7-5.

Figure 7-5. Sample network topology



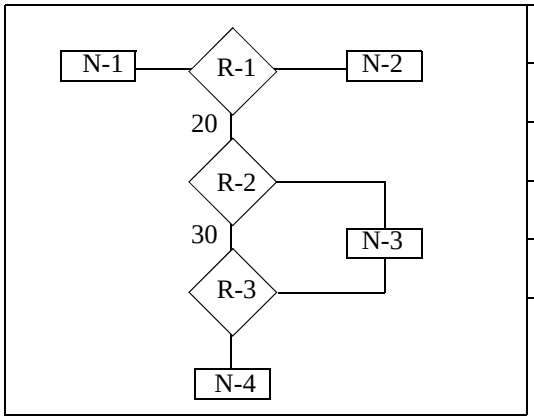
The routers then use the trees to build their routing tables, as shown in Table 7-1.

Table 7-1. Link-state databases for network topology in Figure 7-5

Router-1	**Router-2**	**Router-3**
Network-1/Cost 0	Network-2/Cost0	Network-3/Cost 0
Network-2/Cost 0	Network-3/Cost0	Network-4/Cost 0
Router-2/Cost 20	Router-1/Cost 20	Router-2/Cost 30
	Router-3/Cost 30	

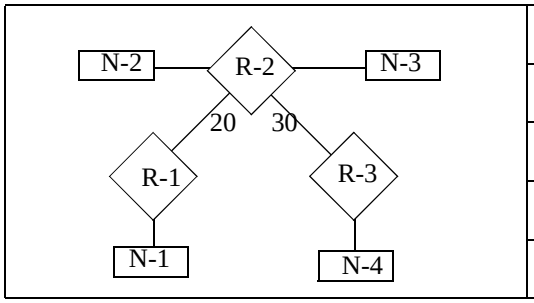
Table 7-2, Table 7-3, and Table 7-4 show another example of self-rooted shortest-path trees calculated from link-state databases, and the resulting routing tables. Actual routing tables also contain externally derived routing data, which is advertised throughout the AS but kept separate from the link-state data. Also, each external route can be tagged by the advertising router, enabling the passing of additional information between routers on the boundary of the AS.

Table 7-2. Shortest-path tree and resulting routing table for Router-1



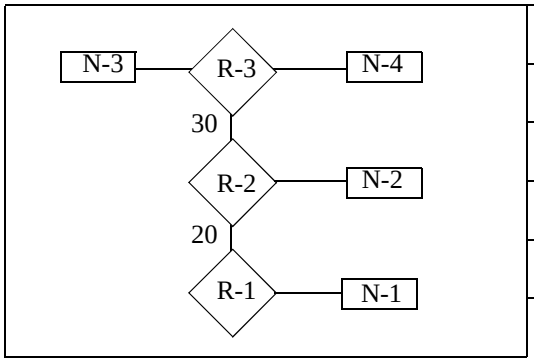
Destination	*Next Hop*	*Metric*
Network-1	Direct	0
Network-2	Direct	0
Network-3	Router-2	20
Network-4	Router-2	50

Table 7-3. Shortest-path tree and resulting routing table for Router-2



Destination	*Next Hop*	*Metric*
Network-1	Router-1	20
Network-2	Direct	0
Network-3	Direct	0
Network-4	Router-2	30

Table 7-4. Shortest-path tree and resulting routing table for Router-3



Destination	*Next Hop*	*Metric*
Network-1	Router-2	50
Network-2	Router-2	30
Network-3	Direct	0
Network-4	Direct	0

Configuring OSPF routing in the DSL Terminator

Following are the parameters related to OSPF routing in the DSL Terminator. (The settings shown are examples.)

```
Ethernet
  Mod Config
```

```
    OSPF options...
      RunOSPF=Yes
      Area=0.0.0.0
      AreaType=Normal
      HelloInterval=10
      DeadInterval=40
      Priority=5
      AuthType=Simple
      AuthKey=lucent0
      Cost=1
      ASE-type=N/A
      ASE-tag=N/A
      TransitDelay=1
      RetransmitInterval=5
    OSPF global options...
      Enable ASBR=Yes
Ethernet
  Connections
    90-101 Cprofile1
      OSPF options...
        RunOSPF=Yes
        Area=0.0.0.0
        AreaType=Normal
        HelloInterval=40
        DeadInterval=120
        Priority=5
        AuthType=Simple
        AuthKey=lucent0
        Cost=10
        ASE-type=N/A
        ASE-tag=N/A
        TransitDelay=5
        RetransmitInterval=20
Ethernet
  Static Rtes
    90-401 SRprofile1
      LSA-type=ExternalType1
```

Understanding the OSPF routing parameters

This section provides some background information about the OSPF parameters. (For detailed information about each parameter, see the *DSL Terminator Reference*.)

Notice that the same configuration parameters appear in Ethernet > Mod Config > OSPF Options and Ethernet > Connections > OSPF Options. The parameters are the same, but some of the default values are different. For OSPF routing, you set the following parameters:

:

Parameter	Description
RunOSPF	Enables/disables OSPF. To enable OSPF on the interface, set RunOSPF to Yes. OSPF is off by default.
Area	Area number in dotted-decimal notation. Note that an area number is not an IP address, although they share the same format. For a description of areas, see “Hierarchical routing (areas)” on page 7-5.
AreaType	Sets the type of area. Specify Normal, Stub, or StubNoDefault. The default setting is Normal, which specifies that external routes are advertised throughout the AS. For additional information, see “Stub areas” on page 7-6.
HelloInterval	Specifies how frequently, in seconds, the DSL Terminator sends out Hello packets on the specified interface. OSPF routers use Hello packets to dynamically detect neighboring routers in order to form adjacencies. The default value is 30 seconds.
DeadInterval	Specifies how many seconds the DSL Terminator waits before declaring its neighboring routers down after it stops receiving their Hello packets. (For background information on Hello packets, see “Exchange of routing information” on page 7-3.)
Priority	Specifies the priority value used to elect a Designated Router (DR) and Backup Designated Router (BDR). A setting of 1 or greater places the DSL Terminator on the list of possible DRs. A setting of 0 excludes the DSL Terminator from becoming a DR/BDR. The higher the priority value of the DSL Terminator relative to other OSPF routers on the network, the better the chances that it will become a BDR/DR For a discussion of the functions of DRs and BDRs, see “Designated and Backup Designated Routers” on page 7-4.
AuthType	Type of authentication to use for validating OSPF packet exchanges. Specify one of the following values: • None—no authentication is required. • Simple—the router uses the password supplied in the Auth-Key parameter to validate OSPF packet exchanges (the default). • MD5—the router uses MD5 encryption and the authentication Key ID supplied in the Key-ID parameter to validate OSPF packet exchanges.
Auth Key	Secret key for authenticating traffic in the router’s area. For more information, see “Security” on page 7-2.
Cost	Cost of routing to the interface. The lower the cost, the higher the likelihood of using that route to forward traffic. For more information, see “Configurable metrics” on page 7-4.

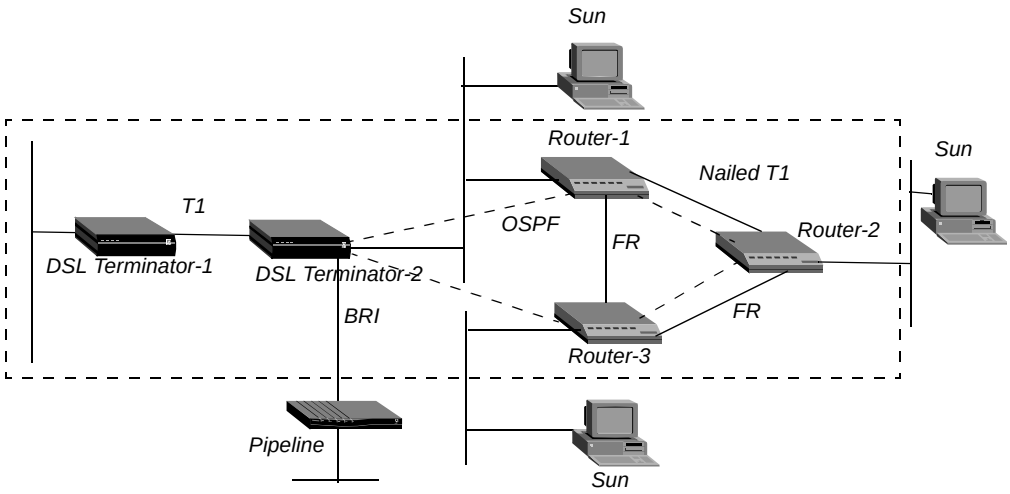
Parameter	Description
ASE-Type	Specifies the type of metric that the DSL Terminator advertises for external routes. Autonomous System External (ASE) routes are used only when OSPF is turned off on a particular interface. When OSPF is enabled, the ASE parameters do not apply. A Type-1 external metric is expressed in the same units as the link-state metric (the same units as interface cost). A Type-2 external metric is considered larger than any link- state path. Use of Type-2 external metrics 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. Used only when OSPF is turned off on a particular interface. When OSPF is enabled, the parameter does not apply.
ASE-Tag	The hexadecimal number used to tag external routes for filtering by other routers.
LSA-Type	Specifies the type of OSPF ASE Link-State Advertisement (LSA). Specify one of the following values: • ExternalType-1—Expressed in the same units as the link-state metric (the same units as interface cost). The default is Type-1. • ExternalType-2—Considered larger than any other link state path. Use of Type-2 external metrics 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. • Internal—Indicates that the static route should be advertised in an internal LSA. The DSL Terminator advertises the static route only if the Static Route gateway has a corresponding entry in a Connection profile. When you set LSA-Type to Internal, the internal LSA static route appears as a stub area to external OSPF routers.
TransitDelay	Specifies the estimated number of seconds it takes to transmit a Link State Update Packet over this interface, taking into account transmission and propagation delays. On a connected route, you can leave the default of 1.
RetransmitInterval	Specifies the number of seconds between retransmissions of Link-State Advertisements, Database Description, and Link State Request Packets.

Parameter	Description
Enable ASBR	Enables or disables Autonomous System Border Routers (ASBRs) in the OSPF Global Options submenu. The calculations are related to external routes. The DSL Terminator imports external routes from RIP (such as when it establishes a WAN link with a caller that does not support OSPF) and performs the ASBR calculations. To prevent the DSL Terminator from performing ASBR calculations, set Ethernet > Mod Config > OSPF Global Options > Enable ASBR to No.

Examples of configurations for adding the DSL Terminator to an OSPF network

This section shows how to add a DSL Terminator to your OSPF network. It assumes that you are familiar with configuring the DSL Terminator with an appropriate IP address as described in Chapter 6, "Configuring IP Routing." The procedures in this section are examples based on Figure 7-6. To apply one or more of the procedures to your network, replace the settings shown with the appropriate values.

Figure 7-6. Example of an OSPF setup



In Figure 7-6, all OSPF routers are in the same area (the backbone area), so the units all form adjacencies and synchronize their databases together.

Note: All OSPF routers in Figure 7-6 have RIP turned off. OSPF can learn routes from RIP without the added overhead of running RIP.

Configuring OSPF on the Ethernet interface

The DSL Terminator Ethernet interface in Figure 7-6 is in the OSPF backbone area. Although there is no limitation stated in the RFC about the number of routers in the backbone area, you should keep the number of routers relatively small, because changes that occur in area zero are propagated throughout the AS.

Another way to configure the same units would be to create a second area (such as 0.0.0.1) on one of the existing OSPF routers and add DSL Terminator-1 to that area. You could then assign the same area number (0.0.0.1) to all OSPF routers reached through the DSL Terminator across a WAN link.

After you configure DSL Terminator-1 as an IP host on that interface, you can configure it, in the Ethernet profile, as an OSPF router in the backbone area. To configure DSL Terminator-1 as an OSPF router on Ethernet:

1 Open Ethernet > Mod Config > Ether Options, and make sure the DSL Terminator is configured as an IP host. For example:

```
Ethernet
  Mod Config
    Ether options...
      IP Adrs=10.168.8.17/24
      2nd Adrs=0.0.0.0
      RIP=Off
      Ignore Def Rt=Yes
      Proxy Mode=Always
      Filter=0
    IPX Frame=N/A
```

Note that RIP is turned off because it is not necessary to run both RIP and OSPF. Turning RIP off reduces processor overhead. OSPF can learn routes from RIP, incorporate them in the routing table, assign them external metrics, and tag them as external routes. (For more information, see Chapter 6, “Configuring IP Routing.”)

2 Open Ethernet > Mod Config > OSPF Options and turn on RunOSPF:

```
RunOSPF=Yes
```

3 Specify the area number and area type for the Ethernet:

```
Area=0.0.0.0
AreaType=Normal
```

In this case, the Ethernet is in the backbone area. (The backbone area number is always 0.0.0.0.) Because the backbone area is not a stub area, leave the setting at its default. (For background information, see “Stub areas” on page 7-6.)

4 Leave the HelloInterval, DeadInterval, and Priority values set to their defaults:

```
HelloInterval=30
DeadInterval=30
Priority=5
```

5 If access to the backbone area requires authentication, specify the password. For example:

```
AuthType=Simple
AuthKey=lucent0
```

If no authentication is required, set AuthType to None.

6 Configure the cost for the DSL Terminator to route into the backbone area. For example:

```
Cost=1
```

Specify a value greater than 0 (zero) and less than 16777215. By default, the cost of an Ethernet-connected route is 1.

7 Set the expected transit delay for Link State Update packets. For example:

```
TransitDelay=1
```

8 Specify the retransmit interval for OSPF packets. For example:

```
RetransmitInterval=5
```

9 Close the Ethernet profile.

When you close the Ethernet profile, the DSL Terminator comes up as an OSPF router on that interface. It forms adjacencies and begins building its routing table.

Configuring OSPF across the WAN

The WAN interface of the DSL Terminator is a point-to-point network. A point-to-point network is any network that joins a single pair of routers. Such networks typically do not provide a broadcasting or multicasting service, so all advertisements are sent point to point.

An OSPF WAN link has a default cost of ten. You can assign a higher cost to reflect a slower connection or a lower cost to set up a preferred route to a certain destination. If the cost of one route is lower than that of another to the same destination, the DSL Terminator does not select the higher-cost route unless route preferences change the equation.

OSPF on the WAN link is configured in a Connection profile. In this example, the DSL Terminator is connecting to another DSL Terminator unit across a T1 link (as in Figure 7-6 on page 7-12). To configure this interface:

1 Open the Connection profile for the remote DSL Terminator unit.

2 Turn on Route IP and configure the IP routing connection. For example:

```
Ethernet
  Connections
    90-101 Cprofile1
      IP options...
        LAN Adrs=10.2.3.4/24
        WAN Alias=0.0.0.0
        IF Adrs=0.0.0.0
        Metric=7
        Preference=N/A
        Private=No
        RIP=Off
        Pool=0
```

(For detailed information, see Chapter 7, “Configuring OSPF Routing.”)

3 Open the OSPF Options subprofile and configure RunOSPF:

```
RunOSPF=Yes
```

4 Specify the area number for the remote device and the area type.

Specify the area number in dotted-quad format, similar to than of an IP address. For example:

```
Area=0.0.0.0
AreaType=Normal
```

You must use the same area number for the Ethernet interface of the DSL Terminator and each of its WAN links. In this example, the Ethernet interface is in the backbone area (0.0.0.0). You can use any area numbering scheme that is consistent throughout the AS and that uses this format.

5 Leave the HelloInterval, DeadInterval, and Priority values set to their defaults.

```
HelloInterval=30
DeadInterval=120
Priority=5
```

Use the Priority value to configure the DSL Terminator as a DR or BDR.

6 If you require authentication to get into the backbone area, specify the password. For example:

```
AuthType=Simple
AuthKey=lucent0
```

If no authentication is required, set AuthType to None.

7 Configure the cost for the route to DSL Terminator-2.

For example, for a T1 link, enter a cost of at least 10.

```
Cost=10
```

8 Close the Connection profile.

9 Reset the DSL Terminator to bring up OSPF.

Note: The remote DSL Terminator unit must also have a comparable Connection profile to connect to DSL Terminator-1.

Configuring a WAN link that does not support OSPF

In this example, the DSL Terminator has a Connection profile to a remote Pipeline unit across a BRI link (as in Figure 7-6 on page 7-12). The remote Pipeline is an IP router that uses RIP-v2 to transmit routes. The route to the Pipeline unit's network, and any routes the DSL Terminator learns about from the remote Pipeline, are ASEs (external to the OSPF system).

To enable OSPF to add the RIP-v2 routes to its routing table, configure RIP-v2 normally in this Connection profile. OSPF imports all RIP routes as Type-2 ASEs.

In this example, RIP is turned off on the link and ASE information is configured explicitly.

1 Open the Connection profile for the remote Pipeline unit.

2 Turn on Route IP and configure the IP routing connection. For example:

```
Ethernet
  Connections
    90-101 Cprofile1
      IP options...
        LAN Adrs=10.2.3.4/24
        WAN Alias=0.0.0.0
        IF Adrs=0.0.0.0
        Metric=7
        Preference=N/A
        Private=No
        RIP=Off
        Pool=0
```

For detailed information, see Chapter 6, "Configuring IP Routing". Note that in a Connection profile, the OSPF Options subprofile includes two ASE parameters that are active only when OSPF is *not* running on a link. If you configure these parameters, the route configured in the Connection profile is advertised whenever the DSL Terminator is up.

3 Open the OSPF Options subprofile.

4 Leave RunOSPF set to No.

```
RunOSPF=No
```

5 Configure the cost for the route to the remote Pipeline.

For example, a single-channel BRI link could have a cost approximately 24 times the cost of a dedicated T1 link:

```
Cost=240
```

6 Specify the ASE type for this route.

```
ASE-type=Type 2
```

7 Enter an ASE tag for this route:

```
ASE-tag=cfff8000
```

8 Close the Connection profile.

Note: The remote Pipeline unit must also have a comparable Connection profile to connect to the DSL Terminator.

Configuring the DSL Terminator as an NSSA internal router

Because the DSL Terminator cannot be an Area Border Router, when you configure OSPF on the DSL Terminator keep in mind that:

- The area type must be the same on all DSL Terminator interfaces running OSPF.
- The area ID (configured in the Area parameter) must be the same on all DSL Terminator interfaces running OSPF.

To configure the DSL Terminator as an NSSA internal router:

1 Select Ethernet > Mod Config > OSPF options.

2 Set AreaType to NSSA.

3 Exit and save the Mod Config profile.

4 Select Ethernet > Static Rtes > *any profile*.

5 Configure a static route to the destination outside the NSSA. For example:

```
Ethernet
  Static Rtes
    90-401 Static Rtes profile 1
      Name=
      Active=Yes
      Dest=20.20.20.20
      Gateway=10.10.10.10
      ...
      ...
      NSSA-ASE7=Advertise
```

Note: To specify whether you want to advertise this route outside the NSSA, set the NSSA-ASE7 parameter to Advertise or to DoNotAdvertise. The settings for the remaining parameters depend on your environment.

```
      Metric=
      Preference=
      Private=
      Ospf-Cost=
      LSA-type=
      ....
```

```
ASE-tag=
Third-Party=
```

6 Exit and save the Static Rtes profile.

Reset the DSL Terminator.

Configuring Packet Bridging

8

Introduction to bridging 8-1
Establishing a bridged connection 8-2
Enabling bridging 8-3
Managing the bridge table 8-3
Bridged IP routing 8-11

Introduction to bridging

Bridging is useful primarily to provide connectivity for protocols other than IP, although it can also be used for joining segments of an IP network. Because a bridging connection forwards packets at the hardware-address level (link layer), it does not distinguish between protocol types, and it requires no protocol-specific network configuration.

The most common uses of bridging in the DSL Terminator are to:

- Provide nonrouted protocol connectivity with another site
- Link two sites so that their nodes appear to be on the same LAN
- Support protocols, such as BOOTP, that depend on broadcasts to function

Disadvantages of bridging

Bridges examine *all* packets on the LAN (in what is termed *promiscuous mode*), so they incur greater processor and memory overhead than routers. On heavily loaded networks, this increased overhead can result in slower performance.

Bridges have other disadvantages. Bridges do not allow the examination of packets at the network layer (instead of the link layer), you cannot filter using logical addresses. Routers support the use of filters that use logical addresses, providing enhanced security and control. In addition, bridges do not support multiple transmission paths to a given destination; routers do, enhancing the reliability and performance of packet delivery.

Note: If you have a DSL Terminator running Multiband Simulation, disable bridging.

Initiating a bridged WAN connection

When you configure the DSL Terminator for bridging, it accepts all packets on the Ethernet and forwards only those that have one of the following:

- A physical address that is not on the local Ethernet segment (the segment to which the DSL Terminator connects)
- A broadcast address

Note: Bridging connections operate on only the physical and broadcast addresses, not on logical (network) addresses.

Physical addresses and the bridge table

A physical address is a unique, hardware-level address associated with a specific network controller. A device's physical address is also called its Media Access Control (MAC) address. On the Ethernet, the physical address is a six-byte hexadecimal number assigned by the Ethernet hardware manufacturer, for example, 0000D801CFF2.

When the DSL Terminator receives a packet whose destination MAC address is not on the local network, it first checks its internal bridge table. (For a description of the table, see "Transparent bridging" on page 8-4.) If the packet's destination MAC address is in its bridge table, the DSL Terminator forwards the packet appropriately.

If the address is *not* specified in its bridge table, the DSL Terminator checks for active sessions that have bridging enabled. If there are one or more active bridging links, the DSL Terminator forwards the packet across *all* active sessions that have bridging enabled.

Broadcast addresses

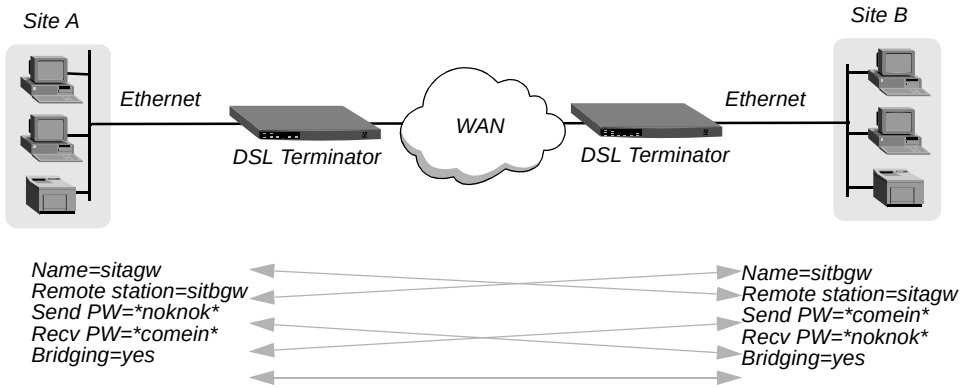
Multiple nodes in a network recognize a broadcast address. For example, the Ethernet broadcast address at the physical level is FFFFFFFFFFFF.

All devices on the same network receive all packets with that destination address. The DSL Terminator discards broadcast packets when you configure the DSL Terminator as a router only. When you configure the DSL Terminator as a bridge, it forwards packets with the broadcast destination address across all active sessions that have bridging enabled.

Establishing a bridged connection

The DSL Terminator uses station names and passwords to synchronize a bridging connection, as shown in Figure 8-1.

Figure 8-1. Negotiating a bridge connection (PPP encapsulation)



The system name assigned to the DSL Terminator in the Name parameter of System > Sys Config must *exactly* match the device name specified in the Connection profile on the remote bridge, as the value entered is case sensitive. Similarly, the name assigned to the remote bridge must exactly match the name specified in the Station parameter of that Connection profile, including case changes.

Note: The most common cause of trouble when initially setting up a PPP bridging connection is specifying the incorrect name for the DSL Terminator or the remote device. Errors often include the case of a character not matching or not entering a dash, space, or underscore.

Enabling bridging

The DSL Terminator has a systemwide bridging parameter that you must enable for any bridging connection to work. The Bridging parameter directs 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. (Even if no packets are actually bridged, running in promiscuous mode incurs greater processor and memory overhead than the standard mode of operation for the Ethernet controller.)

You enable packet bridging by opening Ethernet > Mod Config and setting the Bridging parameter to Yes:

```
Ethernet
   Mod Config
      Bridging=Yes
```

Managing the bridge table

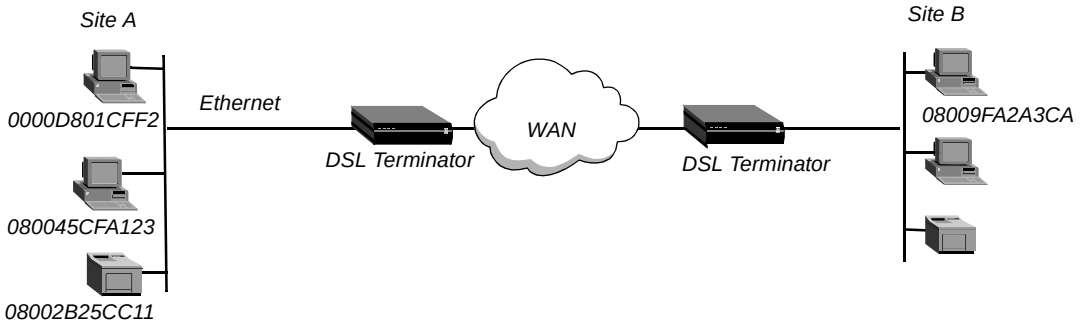
To forward bridged packets to the correct destination network, the DSL Terminator uses a bridge table that associates end nodes with particular connections. It builds this table dynamically (transparent bridging). It also incorporates the entries found in its Bridge Adrs profiles. Bridge Adrs profiles are analogous to static routes in a routing environment. You can define up to 99 destination nodes and their connection information in Bridge Adrs profiles.

Transparent bridging

The DSL Terminator builds a bridge table dynamically (transparent bridging) by looking at each packet's address source. As a transparent bridge (also termed a *learning bridge)*, the DSL Terminator keeps track of the location of a particular MAC address and of the Connection profile that specifies the interface to which the packet should be forwarded. When forwarding a packet, the DSL Terminator logs the packet's source address and creates a bridge table that associates a node address with a particular interface.

For example, Figure 8-2 shows the physical addresses of some nodes on the local Ethernet and at a remote site. The DSL Terminator at Site A has a bridge configuration.

Figure 8-2. How the DSL Terminator *creates a bridging table*



The DSL Terminator at Site A gradually learns addresses on both networks by looking at each packet's source address, and it develops a bridge table that includes the following entries:

```
0000D801CFF2      SITEA
080045CFA123      SITEA
08002B25CC11      SITEA
08009FA2A3CA      SITEB
```

Entries in the DSL Terminator unit's bridge table must be relearned within a fixed aging limit, or they are removed from the table.

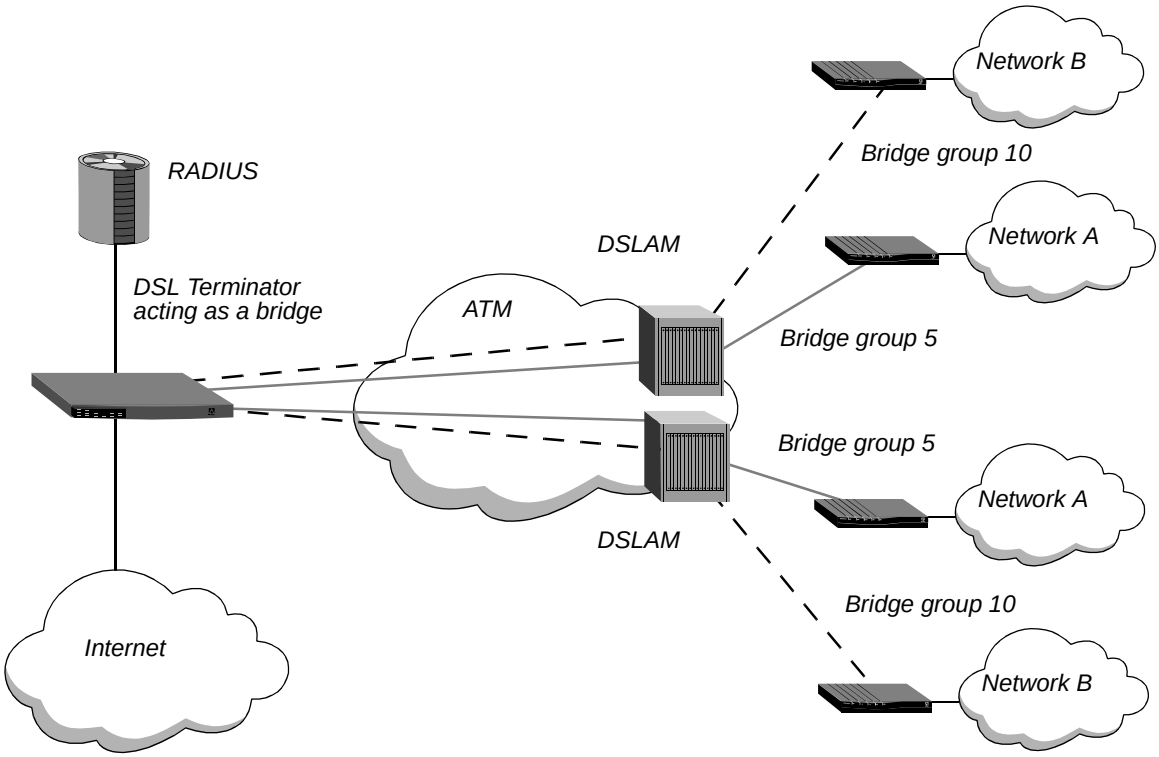
Bridge Groups

Bridge groups enable an administrator to logically group different bridged connections into a single, virtual bridged network. The DSL Terminator unit acts as a bridge between the network segments belonging to the same bridge group, while isolating traffic from networks belonging to different bridge groups. The DSL Terminator Ethernet interfaces can also be configured to belong to a bridge group.

Sample DSL Terminator bridge group configuration

Figure 8-3 shows a sample configuration that uses a bridged, nailed PPP connection between the CPE and the DSL Terminator unit. Network A segments and Network B segments are assigned to different bridge groups. The DSL Terminator acts as bridge for the networks.

Figure 8-3. Example of a DSL Terminator bridge group configuration



Configuration of the setup shown in Figure 8-3 requires the following procedures:

1 Specify bridge groups (including an Ethernet interface, if required).

2 Configure a Connection profile or a RADIUS user profile for each remote site. The profile must specify

- Bridging
- PPP encapsulation
- Nailed call type
- Nailed group that points to the DSL Terminator unit's WAN interface

3 Configure the DSLAM to switch traffic received from the CPE to the DSL Terminator (and vice versa).

4 Configure the CPE device as follows:

- Bridging
- PPP encapsulation

The following subsections describe how to configure a bridge group and a nailed PPP Connection profile on the DSL Terminator unit. For information about configuring the CPE or the DSLAM, see the documentation provided with that unit.

Configuring a bridge group on an Ethernet interface

To configure a bridge group on the Ethernet interface, proceed as follows:

1 Open the Ethernet > Mod Config > Ether1 Options menu. The menu includes the parameters shown in the following example:

```
Mod Config
Ether1 options...
>IP Adrs=204.178.215.151/24
 2nd Adrs=0.0.0.0/0
 RIP=Off
 RIP2 Use Multicast=No
 Ignore Def Rt=Yes
 Proxy Mode=Off
 Filter=0
 Bridge Group=0
 ...
```

2 Specify a bridge group to which this Ethernet interface belongs. For example:

```
Bridge Group=5
```

The unit connects network segments with the same bridge group number.

3 Exit and save the profile.

Configuring the Connection profile for a bridge group

To configure the Connection profile for this example:

1 Open a Connection profile.

2 If configuring a new profile, assign the profile a name. For example:

```
Station=cpe1-bgroup
```

3 Configure the following parameters as shown:

```
Active=Yes
Encaps=PPP
Route IP=No
Bridge=Yes
```

4 Open the Telco Options submenu.

5 Specify that the call is a nailed connection:

```
Call Type=Nailed
```

6 Specify the nailed group number assigned to the WAN interface. For example:

```
Group=32
```

7 Open the Bridge Options submenu.

8 Specify a bridge group. For example:

```
Bridge Group=5
```

To assign this connection to the same bridge group as the Ethernet interface, assign it the same bridge group number you configured in “Configuring a bridge group on an Ethernet interface” on page 8-6.

9 Exit and save the profile.

Configuring additional Connection profiles from existing profiles

Configure the other Connection profiles similarly. To use an existing profile as the basis for a new profile, use the DO Save command as follows:

1 Open the profile you want to copy to another profile.

2 Press Control-D to access the DO menu:

```
>0=Esc
 1=Dial
 P=Password
 S=Save
 E=Termsrv
 D=Diagnostics
```

3 Select `S=Save` and press Enter.

You are prompted to specify the destination profile to which to save the current profile:

```
Save in profile...?
>20-101 cpe1-bgroups
 20-102
 20-103
 20-104
 20-105
..
..
..
```

4 Select the destination profile and press Enter.

The destination profile's contents are replaced with the contents of the open profile.

5 Open the new profile and make the necessary changes for the new connection.

RADIUS user profile for bridge groups

Following is an example of a RADIUS user profile for a bridge group configuration:

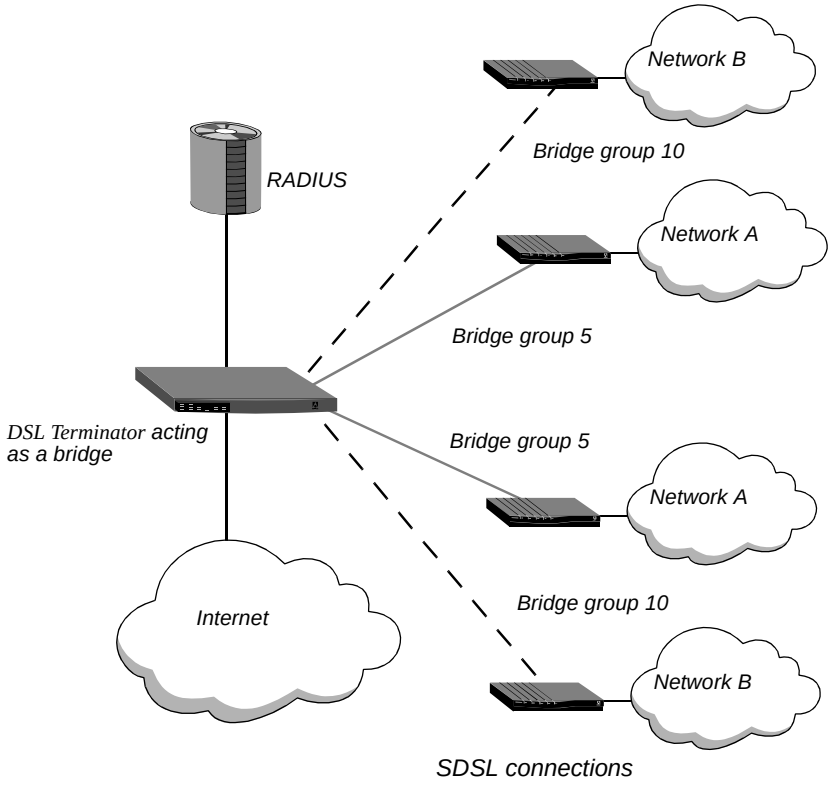
```
permconn-Terminator-1 Password = "ascend"
Service-Type = Outbound,
Framed-Protocol = PPP,
User-Name = "cpe1-radius",
Framed-Routing = None,
Ascend-Call-Type = Nailed,
Ascend-Route-IP = Route-IP-No,
Ascend-Bridge = Bridge-Yes,
Ascend-BIR-Bridge-Group = 5,
Ascend-Group = "32"
```

Example of a DSL Terminator bridge group configuration

Figure 8-4 shows a sample configuration that uses bridged nailed PPP over an SDSL connection between the DSLPipe™ and the DSL Terminator. Network A segments and

Network B segments are assigned to different bridge groups. The DSL Terminator acts as bridge for the networks.

Figure 8-4. Example of a bridge group configuration



Configuration of the setup shown in Figure 8-4 requires the following procedures:

- Specify bridge groups (including an Ethernet interface, if required).
- Configure a Connection profile or a RADIUS user profile for each remote site. The profile must specify
  - Bridging
  - PPP encapsulation
  - Nailed call type
  - Nailed group that points to the DSL Terminator unit's SDSL interface
- Configure the SDSL card as follows:
  - Activate the port
  - Assign a nailed group
- Configure the CPE device as follows:
  - Bridging
  - PPP encapsulation

The following subsections describe how to configure a bridge group and a nailed PPP Connection profile on the DSL Terminator unit. For information about configuring the CPE or the DSLAM, see the documentation that came with that unit.

Configuring a bridge group on an Ethernet interface

To configure a bridge group on the Ethernet interface, proceed as follows:

1 Open the Ethernet > Mod Config > Ether1 Options menu. The menu includes the parameters shown in the following example:

```
Mod Config
Ether1 options...
>IP Adrs=204.178.215.151/24
 2nd Adrs=0.0.0.0/0
 RIP=Off
 RIP2 Use Multicast=No
 Ignore Def Rt=Yes
 Proxy Mode=Off
 Filter=0
 Bridge Group=0
 ...
```

2 Specify a bridge group to which this Ethernet interface belongs. For example:

`Bridge Group=5`

The unit connects network segments with the same bridge group number.

3 Exit and save the profile.

Configuring the SDSL profile

To configure the SDSL card:

1 Open the Net/SDSL> Line Config > Factory profile.

2 Open a Line profile.

3 Enable the port:

`Enabled=Yes`

4 Assign this port to a nailed group:

`Nailed-group=9`

This nailed group is used by the Connection profile which you will configure next.

5 Exit and save the profile.

Configure SDSL profiles for the other networks similarly.

Configuring the Connection profile

To configure the Connection profile for this example:

1 Open a Connection profile.

2 If configuring a new profile, assign the profile a name. For example:

`Station=cpe1-bgroup`

3 Configure the following parameters as shown:

```
Active=Yes
Encaps=PPP
Route IP=No
Bridge=Yes
```

4 Open the Telco Options submenu.

5 Specify that the call is a nailed connection:

```
Call Type=Nailed
```

6 Specify the nailed group number assigned to the SDSL interface. For example:

```
Group=9
```

7 Open the Bridge Options submenu.

8 Specify a bridge group. For example:

```
Bridge Group=5
```

If you want this connection to belong to the same bridge group as the Ethernet interface, assign it the same bridge group number you configured in “Configuring a bridge group on an Ethernet interface” on page 8-9.

9 Exit and save the profile.

Configuring additional Connection profiles from existing profiles

Configure the other Connection profiles example similarly. To use an existing profile as the basis for a new profile, use the DO Save command as follows:

1 Open the profile you want to copy to another profile.

2 Press Control-D to access the DO menu:

```
>0=Esc
 1=Dial
 P=Password
 S=Save
 E=Termsrv
 D=Diagnostics
```

3 Select `S=Save` and press Enter.

You are prompted to specify the destination profile to which to save the current profile:

```
Save in profile...?
>20-101 cpe1-bgroups
 20-102
 20-103
 20-104
 20-105
..
```

4 Select the destination profile and press Enter.

The destination profile’s contents are replaced with the contents of the open profile.

5 Open the new profile and make the necessary changes for the new connection.

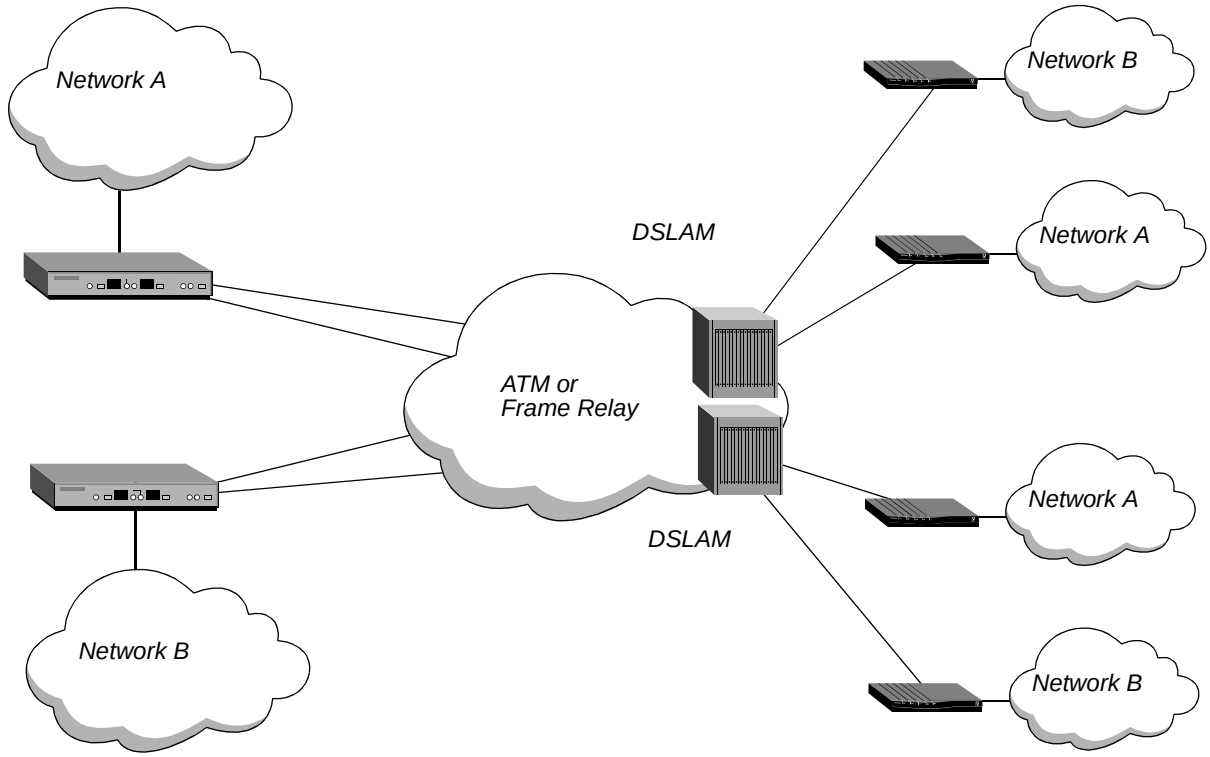
Bridged IP routing

In a Bridged IP Routing (BIR) configuration, the CPEs and DSLAMs use bridging as an encapsulation transport. Once the DSL Terminator receives the traffic, it unencapsulates it and routes it to its destination. Bridged IP routing supports PPP, Frame Relay, and ATM connections.

Overview of bridged IP routing

In a typical DSL environment (Figure 8-5), DSL CPE devices are bridges that are connected to DSLAMs, which act as bridges or switches. The DSLAM connects (over an ATM or Frame Relay network) to a router, which routes the traffic to its destination.

Figure 8-5. DSL bridged environment



A large number of users on such a bridged network can result in excessive number of bridge frames being forwarded throughout the network, possibly reducing performance. In addition, without some type of filtering, traffic can be forwarded on to networks for which it is not intended, compromising security.

To alleviates these problems, bridged IP routing implements a hybrid architecture encapsulating IP traffic in bridge frames. Using bridged IP routing, service providers can concentrate traffic received from sites belonging to the same network into a single PVC or VPI. Traffic from each network is isolated from the other networks.

The DSL Terminator supports these following different bridged IP routing configurations:

- bridged IP routing with subnets

- bridged IP routing with host routes (BIR/32)

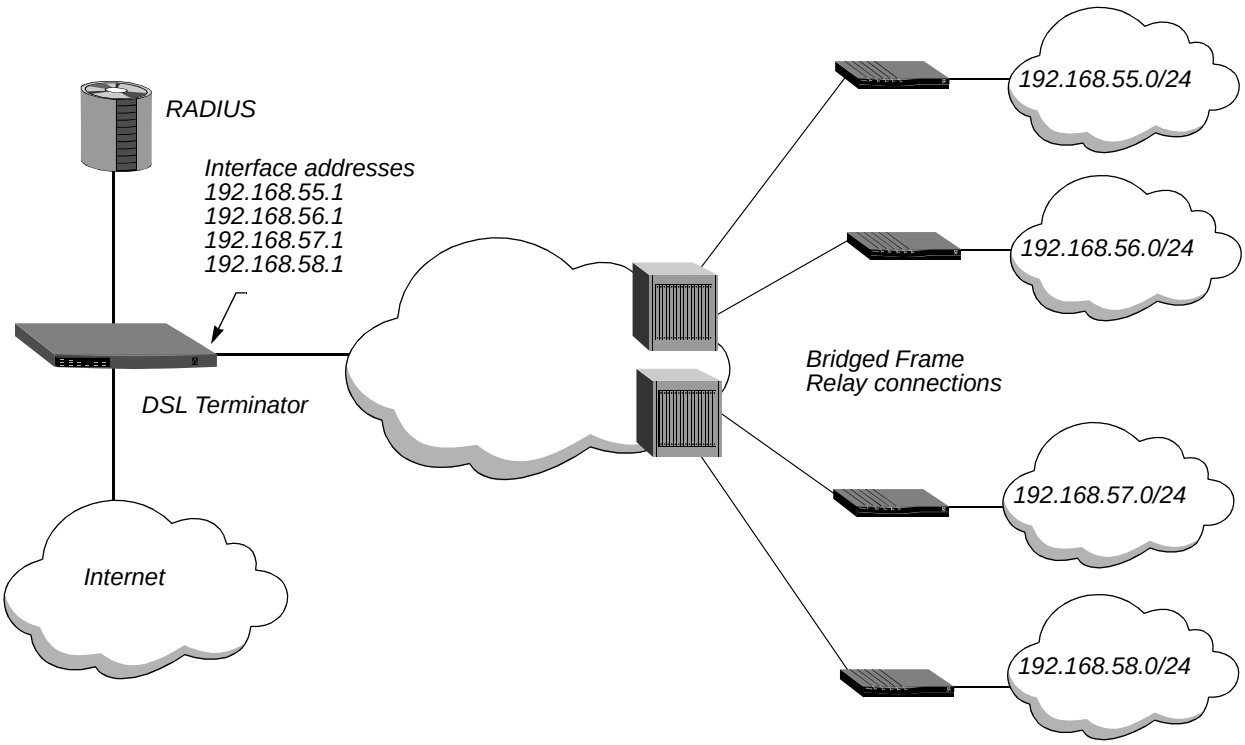
In a bridged IP routing with subnets configuration, different customer networks are assigned to IP subnets and the DSL Terminator has an interface address on each subnet. The unit acts as a router between the networks. Although you can configure the DSL Terminator to connect the networks, Bridged frames from the different networks are isolated from one another.

In a bridged IP routing with host routes (BIR/32) configuration, each remote user is assigned a single IP address (also known as a host route) and the DSL Terminator has a single interface address configured as the gateway for all remote users. The DSL Terminator acts as the router for the entire network of remote users.

Example of a DSL Terminator bridged IP routing with subnets configuration

Figure 8-6 shows a sample configuration that uses a bridged Frame Relay connection between the CPE and a DSL Terminator. Each CPE is on a different network, and the DSL Terminator is the gateway for each network.

Figure 8-6. Sample bridged IP routing with subnets configuration



Configuration of a bridged IP routing with subnets connection like the one in Figure 8-6 requires the following procedures:

- Configure a Frame Relay profile as follows:
  - Specify a name for the profile.
  - Specify the DCE link type.

- Configure a Connection profile or a RADIUS user profile for each remote site. Specify the following settings:
  - IP routing
  - An IP address and subnet mask
  - Frame Relay encapsulation
  - Frame Relay profile name and DLCI
  - RIP updates turned off
  - Bridged IP routing enabled
- Configure the CPE device as follows:
  - Bridging only
  - Nailed Framed Relay connection

The following subsections explain how to configure Frame Relay and Connection profiles on the DSL Terminator unit in Figure 8-6. For information about configuring the CPE, see the documentation that came with the unit.

Configuring the Frame Relay profile

To configure the Frame Relay profile:

1 If configuring a new profile, assign the profile a name. For example:

```
Name=frame-relay1
```

2 Enable the profile:

```
Active=Yes
```

3 Set the Call Type to nailed.

```
Call Type=Nailed
```

4 Set FR type to DCE:

```
FR Type=DCE
```

5 Assign the Frame Relay profile to a nailed-up group. For example:

```
Nailed Grp=1
```

The number you assign must be the same as the number assigned to the DSL Terminator WAN interface. The nailed group must be unique for each active WAN interface.

6 Exit and save the profile.

Configure Frame Relay profiles for the other networks similarly.

Configuring a Connection profile

To configure a Connection profile:

1 Open a Connection profile.

2 If configuring a new profile, assign the profile a name. For example:

```
Station=cpe1-bir
```

3 Configure the following parameters as shown:

```
Active=Yes
Encaps=FR
Route IP=Yes
```

4. Open the IP options submenu.
5. Specify an IP address for a host on the remote network. For example:

   ```
   LAN Adrs=192.168.55.2/24
   ```

6. Verify that the unit does not transmit or receive RIP updates on this connection:

   ```
   RIP=Off
   ```

7. Specify an IP address for the unit's local interface. For example:

   ```
   IF Adrs=192.168.55.1/24
   ```

   This address is the gateway for the remote network.
8. Open the Encaps options submenu.
9. Specify a DLCI and the name of the Frame Relay profile this connection will use. For example:

   ```
   FR Prof=frame-relay1
   DLCI=16
   ```

10. Open the BIR Options submenu.
11. Enable bridged IP routing for this profile:

    ```
    Enabled=Yes
    ```

12. Exit and save the profile.

Configure Connection profiles for the other networks similarly.

RADIUS user profile for bridged IP routing with subnets

Following is a sample configuration of a RADIUS user profile for bridged IP routing with subnets:

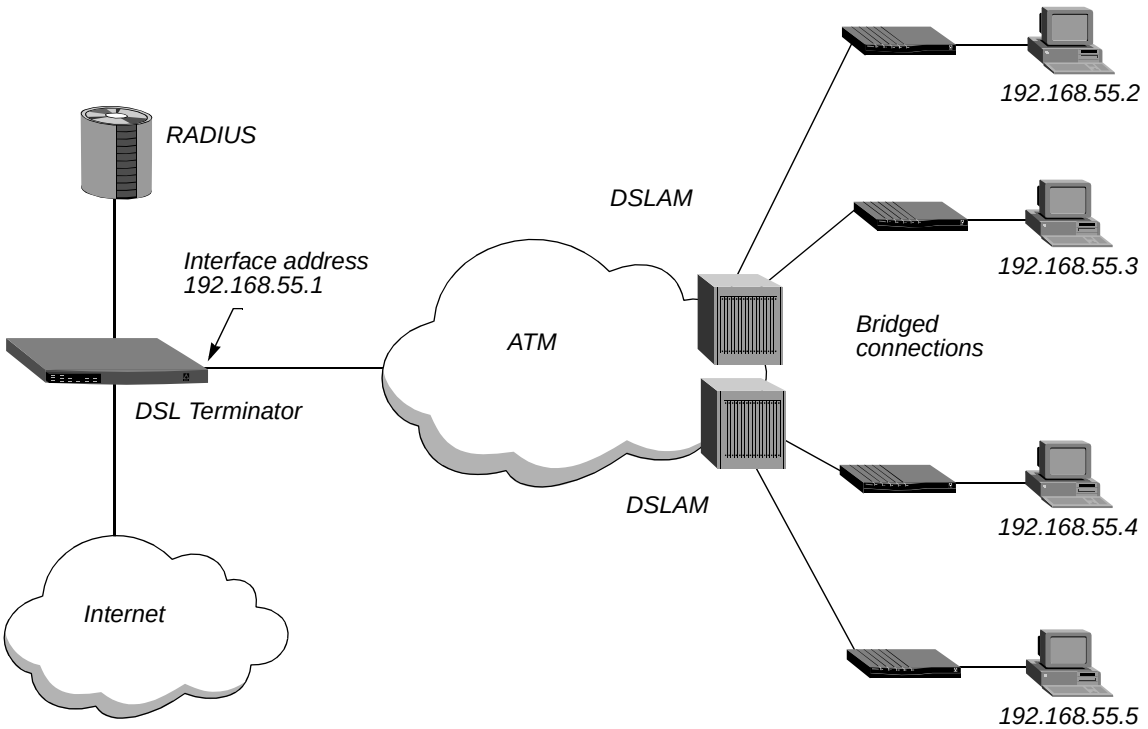
```
permconn-Terminator-1 Password = "ascend"
Service-Type = Outbound,
Framed-Protocol = FR,
Ascend-Call-Type = Nailed,
User-Name = "cpe1-bir",
Framed-Routing = None,
Framed-IP-Address = 192.168.55.2,
Framed-IP-Netmask = 255.255.255.0,
Ascend-Route-IP = Route-IP-Yes,
Ascend-PPP-Address = 192.168.55.1,
Ascend-IF-Netmask = 255.255.255.0,
Ascend-BIR-Enable = BIR-Enable-Yes,
Ascend-FR-DLCI = 16,
Ascend-FR-Profile-Name = "frame-relay1"
```

Example of a DSL Terminator bridged IP routing with host routes configuration

In a bridged IP routing with host routes (BIR/32) configuration (Figure 8-7), each remote user is assigned a single IP address (also known as a host route) and the DSL Terminator has a

single interface address configured as the gateway for all remote users. The unit acts as the router for the entire network of remote users.

Figure 8-7. Bridged IP routing with host routes (BIR/32)



Configuration of the bridged IP routing (BIR/32) connection in Figure 8-7 requires the following procedures:

- Configure a Connection profile or a RADIUS user profile for each remote site. Specify the following settings:
  - IP routing
  - An IP address and subnet mask
  - ATM encapsulation
  - RIP updates turned off
  - Nailed call type
  - Nailed group that points to the DSL Terminator unit's WAN interface
  - An ATM VPI/VCI
  - Bridged IP routing enabled
  - Bridged IP routing proxy ARP enabled
- Configure the DSLAM to switch Frame Relay traffic received from the CPE to the ATM network (and vice versa).
- Configure each CPE device as follows:
  - Bridging only

– Nailed Frame Relay connection

To add users to this network, add a static route from the DSL Terminator unit's local interface to the remote user.

The following subsections describe how to configure a Connection profile on the DSL Terminator unit in Figure 8-7. For information about configuring the CPE or the DSLAM, see the documentation provided with that unit.

Configuring a Connection profile

To configure a Connection profile for the setup in Figure 8-7:

1 Open a Connection profile.

2 If configuring a new profile, assign the profile a name. For example:

```
Station=cpe1-bir32
```

3 Configure the following parameters as shown:

```
Active=Yes
Encaps=ATM
Route IP=Yes
```

4 Open the IP Options submenu.

5 Specify an IP address for a host on the remote network. For example:

```
LAN Adrs=192.168.55.2/32
```

6 Specify an IP address for the unit's local interface. For example:

```
IF Adrs=192.168.55.1/24
```

This address is the gateway for all the remote users.

7 Open the Encaps submenu:

8 Specify the ATM VPI and VCI for the remote device. For example:

```
vpi=12
vci=101
```

Note: Your ATM service provider should provide the actual values.

9 Open the IP Options submenu.

10 Verify that RIP updates are disabled:

```
RIP=Off
```

11 Open the Telco Options submenu.

12 Set the Call Type parameter to Nailed:

```
Call Type=Nailed
```

13 Specify the nailed group number. For example:

```
Group=32
```

14 Open the BIR Options submenu.

15 Enable bridged IP routing for this profile and specify whether the unit will answer ARP requests for this device:

```
Enabled=Yes
Proxy Arp=Yes
```

16 Exit and save the profile.

17 Configure Connection profiles for the other networks similarly.

RADIUS user profile for bridged IP routing with host routes

Following is an example of a RADIUS user profile for a bridged IP routing with host routes configuration:

```
permconn-Terminator-1 Password = "ascend"
Service-Type = Outbound,
Framed-Protocol = ATM-1483,
User-Name = "cpe1-radius",
Framed-Routing = None,
Framed-IP-Address = 192.168.55.2,
Framed-IP-Netmask = 255.255.255.255,
Ascend-Call-Type = Nailed,
Ascend-Route-IP = Route-IP-Yes,
Ascend-PPP-Address = 192.168.55.1,
Ascend-IF-Netmask = 255.255.255.0,
Ascend-BIR-Enable = BIR-Enable-Yes,
Ascend-BIR-Proxy = BIR-Proxy-Yes,
Ascend-Group = "32",
Ascend-ATM-Vpi=12,
Ascend-ATM-Vci=101
```

Designating egress interfaces for bridged IP routing or bridge groups

On a DSL Terminator that is configured to support bridge groups or bridged IP routing, you can designate an interface to act as an egress (outgoing or sending) interface for bridging packets from specific CPE.

On a conventional Ethernet bridge, broadcast, multicast, and unicast packets arrive at all incoming interfaces. On a DSL Terminator unit configured for bridging and with an interface configured as an egress interface, incoming packets from bridging CPE arrive only at the egress interface.

This method of egress bridge switching isolates packets received from one network segment to one interface, helping to create a secure and manageable network.

Any Ethernet, Frame Relay, ATM, or PPP interface can be configured in its Connection profile as an egress interface.

To designate an interface as an egress interface, set the Designate Egress parameter to yes. The default value is No.

Packets from the egress interface are handled in the conventional manner, as with any multiport Ethernet bridge. Broadcast and multicast packets flood all active interfaces and unicast packets go to the bridge logic for destination-interface lookup. If the destination is found, the packet is sent there. Otherwise, it is flooded onto all active interfaces.

Parameter and RADIUS attribute reference

Bridged IP routing uses the Bridge Group, Enabled, and Proxy ARP parameters.

Bridge Group	Specifies the bridge group assigned to the Ethernet interface (Mod Config profile) or the connection (Connection profile). Bridge groups enables you to group several bridged connections or Ethernet ports into one logical bridge. Specify a number from 0 to 2000.
Enabled (BIR)	Enables or disables bridged IP routing (BIR). Specify Yes or No. No is the default.
Proxy ARP	Specifies the conditions under which the DSL Terminator responds to an ARP request for remote devices. With Proxy ARP parameter enabled, the DSL Terminator responds to the ARP request with its own MAC address. Enable the Proxy ARP parameter under the following conditions: • 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 need not enable Proxy ARP because most routing protocols (including those used over the Internet) are designed to propagate subnet mask information.

Bridged IP routing uses Ascend-BIR-Enabled, Ascend-BIR-Proxy, and Ascend-Bridge-Group attributes.

```
#  BIR Attributes
#
ATTRIBUTE  Ascend-BIR-Enable         71     integer
ATTRIBUTE  Ascend-BIR-Proxy          72     integer
ATTRIBUTE  Ascend-BIR-Bridge-Group   73     integer

#Ascend BIR values
VALUE      Ascend-BIR-Enable   BIR-Enable-No    0
VALUE      Ascend-BIR-Enable   BIR-Enable-Yes   1

VALUE      Ascend-BIR-Proxy    BIR-Proxy-No     0
VALUE      Ascend-BIR-Proxy    BIR-Proxy-Yes    1
```

Restricting multicast bridging

In a typical DSL Terminator configuration, the Lucent unit performs bridging, and all transmission to and from the CPEs are bridged. You can restrict the DSL Terminator unit's ability to bridge multicast packets by specifying whether the hosts on the other side of the WAN are using IP multicast forwarding. Using IGMP, the DSL Terminator forwards multicast frames to the interface only if a host with the same group has been detected on the interface.

To disable multicast bridging, set the Multicast Client parameter to No in Ethernet>Connections>IP options. The Multicast Client parameter does not apply if multicast forwarding is disabled or if the Connection profile is the Mbone profile.

Overview of RADIUS bridging attributes

Table 8-1 lists the bridging attributes.

Table 8-1. Bridging attributes

Attribute	Description	Possible values
Ascend-Bridge (230)	Enables or disables protocol-independent bridging for the call.	Bridge-No (0) Bridge-Yes (1) The default value is Bridge-No.
Ascend-Bridge-Address (168)	Specifies the IP address and associated MAC address of a device on a remote LAN to which the DSL Terminator unit can form a bridging connection. Also specifies the name of the dialout profile the DSL Terminator unit uses to bring up the connection.	`MAC_address` specifies the destination device's hardware address. The default value is 000000000000. `profile_name` specifies the dialout profile that brings up the connection. `IP_address` specifies the destination device's IP address. The default value is 0.0.0.0.

Specifying protocol-independent bridging

To specify that bridging is available to a user profile, follow these steps:

1. Specify the User-Name and Password attributes, authentication attributes, and WAN connection attributes.

   The most common cause of trouble when setting up a bridging connection is specifying the wrong name for the DSL Terminator unit or the remote device. You must specify the name of the remote device or user exactly as it appears remotely, including case changes, dashes, and underscores.

   For details on setting the User-Name, Password, and authentication attributes, see Chapter 2, "Setting Up Security."

2. To turn on bridging for the user profile, set the Ascend-Bridge profile to Bridge-Yes.

Configuring bridge entries

To set up bridge entries in RADIUS for the bridge table, follow these steps:

1. Create the first line of a pseudo-user profile using the User-Name, Password, and User-Service attributes.

   For a unit-specific bridge profile, specify the first line of a pseudo-user profile in this format:

```
Bridge-unit_name-num Password="Ascend", User-Service=
Dialout-Framed-User
```

where `unit_name` is the system name of the DSL Terminator unit—that is, the name specified by the Name parameter in the System profile and `num` is a number in a sequential series, starting at 1.

2 For each pseudo-user profile, specify one or more bridge entries using the Ascend-Bridge-Address attribute.

The Ascend-Bridge-Address attribute has this format:

```
Ascend-Bridge-Address="MAC_address profile_name IP_address"
```

Table 8-2 describes Ascend-Bridge-Address arguments.

Table 8-2. Ascend-Bridge-Address arguments

Argument	Description
`MAC_address`	Specifies a MAC address in standard 12-digit hexadecimal format (yyyyyyyyyyyy) or in colon-separated format (yy:yy:yy:yy:yy:yy). If the leading digit of a colon-separated pair is 0 (zero), you do not need to enter it. That is, `:y` is the same as `:0y`. The default value is 000000000000.
`profile_name`	Specifies the name of the dialout profile the DSL Terminator unit uses to bring up the connection. You can specify either a Connection profile or a RADIUS user profile. The DSL Terminator unit looks for a local profile first.
`IP_address`	Specifies an IP address in dotted decimal notation. The default value is 0.0.0.0.

Each Ascend-Bridge-Address setting specifies the IP address and associated MAC address of a device on a remote LAN to which the DSL Terminator unit can form a bridging connection. When your DSL Terminator unit receives an ARP request for one of the IP addresses you specify, the DSL Terminator unit replies with the corresponding MAC address and uses the specified profile to bring up a connection to that address. Because the DSL Terminator unit replies to these ARP requests as if the IP devices were local, you must have user profiles that bridge IP packets to each device.

Whenever you power on or reset the DSL Terminator unit, or when you select the Upd Rem Cfg command from the Sys Diag menu, RADIUS adds bridging entries to the bridge table in this way:

1 RADIUS looks for profiles having the format Bridge-`unit_name-num,` where `unit_name` is the system name and `num` is a number in a sequential series, starting with 1.

2 RADIUS loads the data to create the bridging tables.

Bridge profile configuration examples

This example creates two bridging table entries.

```
Bridge-Ascend-1 Password="Ascend", User-Service=Dialout-Framed-User
    Ascend-Bridge-Address="2:2:3:10:11:12 Prof1 1.2.3.4 1",
    Ascend-Bridge-Address="2:2:3:13:14:15 Prof2 5.6.7.8 2"
```

Setting Up IP Multicast Forwarding

9

Introduction to multicast forwarding 9-1

Configuring multicast forwarding 9-2

You can configure your DSL Terminator unit to act as a multicast forwarder, responding as a client to IGMP packets from the Multicast Backbone (MBONE) router and acting as an MBONE router by forwarding IGMP queries to clients, receiving their responses, and forwarding multicast traffic.

To configure the unit for this role, you enable multicast forwarding, identify the MBONE router, and identify and configure WAN and LAN interfaces for accepting multicast traffic. Parameters for configuring the multicast system behavior are located in the Ethernet > Mod Configure > Multicast profile. Parameters for configuring WAN interfaces (and the MBONE router identification when it is located across a WAN) are located in Connection profiles for the WAN.

Introduction to multicast forwarding

Video and audio transmissions use one-to-many and many-to-many communication, rather than the point-to-point communications that many other types of network applications use. This type of transmission is provided by the IP Multicast Backbone (MBONE) as a much cheaper and faster way to communicate the same information to multiple hosts.

MBONE routers maintain multicast groups, in which hosts must register to receive a multicast transmission. Multicast group functions are handled using the Internet Group Management Protocol (IGMP). The DSL Terminator forwards IGMP version-1 or version-2 packets, including IGMP MTRACE (multicast trace).

The interface to the MBONE router is the MBONE interface. The DSL Terminator can have one MBONE interface, either a LAN or WAN IP interface, depending on where the MBONE router is located.

When it is configured to act as a multicast forwarder, the DSL Terminator appears to MBONE routers as a multicast client, because it responds as a client to IGMP packets. The DSL Terminator appears to multicast clients to be an MBONE router, because it forwards IGMP queries to those clients, receives their responses, and forwards multicast traffic.

Configuring multicast forwarding

To configure the DSL Terminator to act as a multicast forwarder, enable multicast forwarding and identify the MBONE interface. You also need to configure the local or WAN interfaces that support multicast clients. Depending on your network requirements, you might also want to configure heartbeat monitoring, which provides monitoring for connectivity problems.

Parameters used to configure multicast forwarding are located in the Ethernet > Mod Config > Multicast profile and in Ethernet > Connections > *any Connection profile* > IP Options profiles. For detailed information about each parameter, see the DSL Terminator *Reference.*

Enabling multicast forwarding

To enable multicast forwarding, you must set the Ethernet > Mod Config > Multicast > Forwarding parameter to Yes. When you change the parameter from No to Yes, the multicast subsystem reads the values in the Ethernet profile and initiates the forwarding function.

If you modify any other multicast value in the Ethernet profile, you must set the Forwarding parameter to No and then back to Yes again to force a read of the new value.

Identifying the MBONE interface

The MBONE interface is the one on which the MBONE router resides. If it resides across the WAN, you must set the Ethernet > Mod Config > Multicast > Mbone Profile parameter to specify the name of a Connection profile to connect to that router. If the MBONE router resides on the same LAN as the DSL Terminator unit, you leave the Mbone Profile parameter set to null and the DSL Terminator assumes that its Ethernet is the MBONE interface.

Multicast forwarder polling activities

When you configure the DSL Terminatoras a multicast forwarder, it forwards polling messages generated by the multicast router and keeps track of active memberships from its client interfaces. To configure the timeout value for deactivating memberships, you can set the Ethernet > Mod Config > Multicast > Membership Timeout parameter to a value from 60 to 65535 seconds. The factory default is six minutes.

Configuring the DSL Terminator to support multicast clients

To configure the DSL Terminator to support multicast clients, you need to specify which interfaces should support them, the rate at which the DSL Terminator accepts multicast packets from clients, and how the DSL Terminator responds to IGMP `leave group` messages.

Specifying the interfaces that support multicast clients

Each local or WAN interface that supports multicast clients must have the Ethernet > Mod Config > Multicast > Client parameter set to Yes (or you can set the Multicast Client parameter in each client's Connection profile to Yes). With this setting, the DSL Terminator begins handling IGMP requests and responses on the interface. It does not begin forwarding multicast traffic until you set the Ethernet > Mod Config > Multicast > Rate Limit parameter.

Specifying the rate which multicast clients accept packets

The Rate Limit parameter specifies the rate at which the DSL Terminator accepts multicast packets from its clients. For a particular WAN connection, you can set the Multicast Rate parameter in the Connection profile. The rate limit does not affect the MBONE interface. The default setting is 100, which *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 parameter to a number less than 100. For example, if you set it to 5, the DSL Terminator accepts a packet from multicast clients on the interface once every five seconds. The DSL Terminator discards any subsequent packets received in that five-second window.

Because multiple multicast clients can have multiple active sessions for identical IGMP groups via a single WAN interface on the DSL Terminator, you can configure the DSL Terminator to query each WAN interface from which it receives a `leave group` message, to make sure there are no clients with active multicast sessions for the same group on that interface.

Querying for active group members

When you set a value for the Grp Leave Delay parameter and the DSL Terminator receives a `leave group` message for a WAN interface, the DSL Terminator sends a query to the WAN interface, requesting that any active members of the group respond. If the DSL Terminator receives a response within the time period you specify in the Grp Leave Delay parameter, it does not forward the `leave group` message to the MBONE. Otherwise, it sends a `leave group` message to the MBONE, and it clears the IGMP group session from its tables.

Multicast interfaces

The DSL Terminator creates the following multicast interfaces at system startup:

Interface	Specified destination address
mcast	224.0.0.0/4. All multicast addresses, except for special addresses discussed in this section, are directed to this interface.
local	224.0.0.1/32. Multicast address for all systems on the local subnet. The DSL Terminator does not forward packets sent to this address.
local	224.0.0.2/32. Multicast address for all routers on the local subnet. The DSL Terminator does not forward packets sent to this address.
local	224.0.0.5/32. Multicast address for all OSPF routers on the network. The DSL Terminator does not forward packets sent to this address. If you disable OSPF routing, this route changes from local to a black-hole interface.
local	224.0.0.6/32. Multicast address for all OSPF Designated Routers on the network. The DSL Terminator does not forward packets sent to this address. If you disable OSPF routing, this route changes from local to a black-hole interface.

Implicit priority setting for dropping multicast packets

For high-bandwidth data, voice, and audio multicast applications, the DSL Terminator supports prioritized packet dropping. If the DSL Terminator is the receiving device under extremely high loads, it drops packets according to a priority ranking, determined by the following UDP port ranges:

- Traffic on ports 0–16384 (unclassified traffic) has the lowest priority (50).
- Traffic on ports 16385–32768 (audio traffic) has the highest priority (70).
- Traffic on ports 32769–49152 (whiteboard traffic) has medium priority (60).
- Traffic on ports 49153–65536 (video traffic) has low priority (55).

Monitoring connectivity problems through heartbeat monitoring

When running as a multicast forwarder, the DSL Terminator continually receives multicast traffic. Heartbeat-monitoring is an optional feature enables the administrator to monitor possible connectivity problems by continuously polling for this traffic and generating an SNMP alarm trap in the event of a traffic breakdown. Following is the SNMP alarm trap:

```
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 DSL Terminator
started sending SNMP Alarms (4bytes).
```

To set up heartbeat monitoring, you configure several parameters that define the packets to be monitored, how often and for how long to poll for multicast packets, and the threshold for generating an alarm. Following are the parameters you use to specify these settings:

Setting	Parameters
Packets to be monitored	HeartBeat Address specifies a multicast address. If set, causes the DSL Terminator to listen for packets to and from the specified address.
	HeartBeat UDP Port specifies a UDP port number. If set, causes the DSL Terminator to listen only to packets received through the specified port.
	Source Addr and Source Mask specify an IP address and subnet mask. If you specify an address, the DSL Terminator ignores packets from that source for monitoring purposes.
How often and for how long to poll for multicast packets	HeartBeat Slot Time specifies an interval (in seconds). The DSL Terminator polls for multicast traffic, waits for the duration of the interval, then polls again.
	HeartBeat Slot Count specifies how many times to poll before comparing the number of heartbeat packets received to the Alarm Threshold.

Setting	Parameters
Threshold for generating an alarm	Heartbeat Alarm Threshold specifies a number. If the number of monitored packets falls below this number, the DSL Terminator sends the SNMP alarm trap.

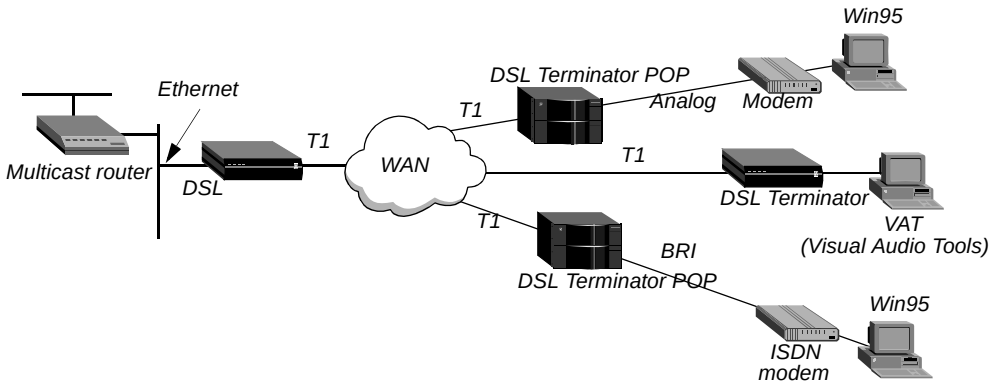
Examples of multicast forwarding configuration

The examples in this section show how to configure MBONE routers on the Ethernet and on a WAN. They also show how to configure multicast clients.

Forwarding from an MBONE router on Ethernet

Figure 9-1 shows a local multicast router on one of the DSL Terminator unit's Ethernet interfaces, and dial-in multicast clients.

Figure 9-1. DSL Terminator forwarding multicast traffic to dial-in multicast clients



Note: Heartbeat monitoring is an optional feature. You can operate multicast forwarding without it if you prefer.

As an example of this type of multicast configuration, the following procedure specifies the MBONE interface as the Ethernet port, and uses the heartbeat group address of 224.1.1.1:

1 Open Ethernet > Mod Config > Multicast and set Forwarding to enable multicast forwarding. Leave the default values for the Mbone Profile, Client, and Rate Limit parameters:

```
Ethernet
   Mod Config
      Multicast...
         Forwarding=Yes
         Membership Timeout=60
         Mbone Profile=
         Client=No
         Rate Limit=5
```

2 Set the HeartBeat Addr and Heartbeat UDP parameters to specify a heartbeat group address and UDP port for monitoring heartbeat packets. For example:

```
HeartBeat Addr=224.1.1.1
HeartBeat Udp Port=16387
```

3 Set the Heartbeat Slot Time, HeartBeat Slot Count, and Alarm Threshold parameters to specify the time, count, and alarm threshold. For example:

```
HeartBeat Slot Time=10
HeartBeat Slot Count=10
Alarm threshold=3
Source Addr=0.0.0.0
Source Mask=0.0.0.0
```

4 Exit the profile and, at the exit prompt, select the `exit and accept` option.

To enable multicasting on WAN interfaces, proceed as follows:

1 Open the Connection profile for a multicast client site.

2 Open the IP Options subprofile and set Multicast Client to Yes. If appropriate, set the Multicast Rate Limit parameter to specify a rate limit other than the default of 5.

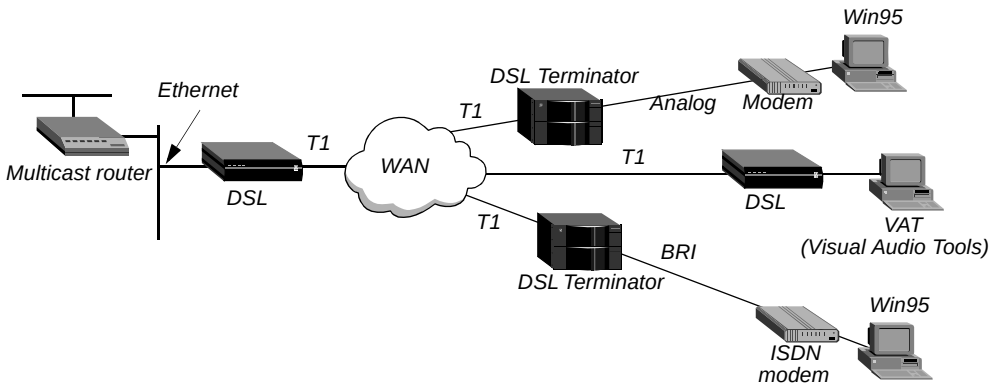
```
Ethernet
   Connections
      0-101 Crofile1
         Ip options...
         Multicast Client=Yes
         Multicast Rate Limit=5
```

3 Exit the profile and, at the exit prompt, select the `exit and accept` option.

Forwarding from an MBONE router on a WAN link

Figure 9-2 shows a multicast router on the WAN with local and dial-in multicast clients. This example presents a sample configuration for the local DSL Terminator unit in the figure. The configuration specifies the MBONE interface as a WAN link accessed through a Connection profile # 4.

Figure 9-2. DSL Terminator forwarding multicast traffic to dial-in multicast clients



Note: Heartbeat monitoring is an optional feature. You can operate multicast forwarding without it if you prefer.

Configuring the DSL Terminator to respond to multicast clients

To configure the DSL Terminator to respond to multicast clients on the Ethernet, proceed as follows:

1 Open Ethernet > Mod Config > Multicast and set the Forwarding parameter to enable multicast forwarding, set Mbone Profile to specify the number of the Connection profile for the MBONE interface, and set Client to Yes:

```
Ethernet
   Mod Config
      Multicast...
         Forwarding=Yes
         Membership Timeout=60
         Mbone Profile=20
         Client=Yes
```

2 In the same profile, set Multicast Rate Limit to a number lower than the default of 100:

```
Rate Limit=5
```

3 Exit the profile and, at the exit prompt, select the `exit and accept` option.

Configuring the MBONE interface

To configure the MBONE interface, proceed as follows:

1 Open the Connection profile for an MBONE interface (in this example, profile # 4).

2 Open the IP options subprofile and set Multicast Rate Limit to a number lower than the default of 100:

```
Ethernet
   Connections
      90-104 Cprofile4
         Ip Options...
            Multicast Client=No
            Multicast Rate Limit=5
```

3 Exit the profile and, at the exit prompt, select the `exit and accept` option.

Configuring multicasting on WAN interfaces

To enable multicasting on WAN interfaces, proceed as follows:

1 Open the Connection profile for a multicast client site.

2 Open the IP options subprofile. Set the Multicast Client parameter to Yes and set the Multicast Rate Limit parameter to a number lower than the default of 100:

```
Ethernet
   Connections
      90-106 Cprofile6
         Ip options...
            Multicast Client=Yes
            Multicast Rate Limit=5
```

3 Exit the profile and, at the exit prompt, select the `exit and accept` option.

Restricting multicast bridging

In a typical DSL Terminator configuration, the DSL Terminator performs bridging, and all transmission to and from the CPEs are bridged. You can restrict the DSL Terminator unit's ability to bridge multicast packets by specifying whether the hosts on the other side of the WAN are using IP multicast forwarding. Using IGMP, the DSL Terminator forwards multicast frames to the interface only if a host with the same group has been detected on the interface.

To restrict multicast bridging, go to Ethernet > Connections > IP options and set the Multicast Client parameter to Yes. The Multicast Client parameter specifies whether hosts on the other side of the WAN are using IP multicasting. The default setting is No. This parameter does not apply if multicast forwarding is disabled or if the Connection profile is the Mbone profile (linking to a remote multicast router).

Setting up multicast forwarding using RADIUS

Before configuring the RADIUS user profile for multicast forwarding, you must set multicast parameters in the Ethernet profile of the DSL Terminator configuration interface.

Configuring multicast forwarding in RADIUS

To configure multicast forwarding in RADIUS, use the attributes listed in Table 9-1.

Table 9-1. Multicast forwarding attributes

Attribute	Description	Possible values
Ascend-Multicast-Client (152)	Specifies whether the user is a multicast client of the DSL Terminator unit.	Multicast-No (0) Multicast-Yes (1) The default value is Multicast-No.
Ascend-Multicast-Rate-Limit (153)	Specifies how many seconds the DSL Terminator unit waits before accepting another packet from the multicast client.	The default value is 100.

To configure a multicast forwarding in a RADIUS user profile, follow these steps:

1. To specify that the user is a multicast client of the DSL Terminator unit, set Ascend-Multicast- Client=Multicast-Yes.
2. To specify how many seconds the DSL Terminator unit waits before accepting another packet from the multicast client, specify a value for Ascend-Multicast-Rate-Limit.

   To prevent multicast clients from creating response storms to multicast transmissions, you configure the user profile to limit the rate at which the DSL Terminator unit accepts packets from clients. Specify an integer. If you set the attribute to 0 (zero), the DSL Terminator unit does not apply rate limiting. The default value is 100. The DSL Terminator unit discards any subsequent packets it receives in the window you configure.

Configuring Virtual Private Networks 10

Introduction to virtual private networks. 10-1

Configuring PPTP tunnels 10-23

Configuring L2TP tunnels 10-27

Configuring Virtual Routers. 10-33

Introduction to virtual private networks

Virtual Private Networks (VPN) provides a low-cost remote access to private LANs using the Internet. The tunnel to the private corporate network can be from an ISP (enabling Mobile Clients to connect to a corporate network), or it can be an Internet connection between two corporate networks. Lucent currently supports the following VPN schemes: Ascend Tunnel Management Protocol (ATMP), Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Tunneling Protocol (L2TP).

An ATMP session can occur only between two Lucent units and must use UDP/IP. The DSL Terminator encapsulates all packets passing through the tunnel in standard Generic Routing Encapsulation (GRE), as described in RFC 1701. ATMP creates and tears down a cross-Internet tunnel between the two Lucent units. In effect, the tunnel collapses the Internet cloud and provides what looks like direct access to a Home network. The tunnels do not support bridging. All packets must be routed with IP.

The Microsoft Corporation developed Point-to-Point-Tunneling Protocol (PPTP) to enable Microsoft Windows 95 and Windows NT Workstation users to dial in to a local ISP to connect to a private corporate network across the Internet.

Version 8 of the Internet Engineering Task Force (IETF) draft titled *Layer Two Tunneling Protocol "L2TP,"* dated November 1997, defines the Layer 2 Tunneling Protocol (L2TP). L2TP enables you to connect to a private network by connecting to a local DSL Terminator, which creates and maintains an L2TP tunnel between itself and the private network.

Note: Any unit supporting PPTP or L2TP does not display a terminal-server prompt to dial-in users because all dial-in calls are immediately transferred to PPTP or L2TP servers.

Creating and Configuring ATMP tunnels

ATMP is a UDP/IP-based protocol for tunneling between two Lucent units across an IP network. Data is transported through the tunnel in Generic Routing Encapsulation (GRE), as

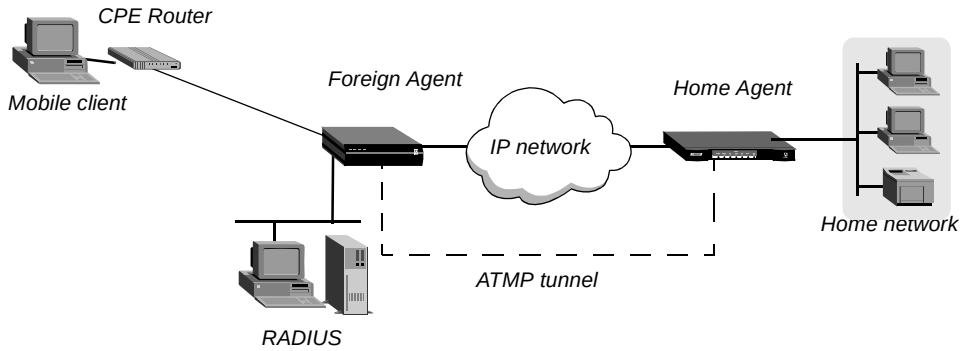
described in RFC 1701. (For a complete description of ATMP, see RFC 2107, *Ascend Tunnel Management Protocol - ATMP.*)

When an ATMP tunnel works between two DSL Terminator units, one of the units acts as a *Foreign Agent* (typically a local ISP) and one as a *Home Agent* (which can access the Home network). A Mobile Client dials in to the Foreign Agent which establishes a cross-Internet IP connection to the Home Agent. The Foreign Agent then requests an ATMP tunnel on top of the IP connection. The Foreign Agent must use RADIUS to authenticate Mobile Clients.

The Home Agent is the terminating part of the tunnel and provides most of the ATMP intelligence. It must be able to communicate with the Home network (the destination network for Mobile Clients) through a direct connection, another router, or across a nailed connection.

For example, in Figure 10-1, the Mobile Client might be a sales person who logs into an ISP to access his or her Home network. The ISP is the Foreign Agent. The Home Agent has access to the Home network.

Figure 10-1. ATMP tunnel across the Internet



How the DSL Terminator creates ATMP tunnels

The DSL Terminator establishes an ATMP connection as follows:

1 A Mobile Client dials a connection to the Foreign Agent.

2 The Foreign Agent uses a RADIUS profile to authenticate the Mobile Client.

The DSL Terminator, configured as a Foreign Agent, requires RADIUS authentication of the Mobile Client, because only RADIUS supports the required attributes.

3 The Foreign Agent uses the Ascend-Home-Agent-IP-Addr attribute in the Mobile Client's RADIUS profile to locate a Connection profile (or RADIUS profile) for the Home Agent.

4 The Foreign Agent connects to the Home Agent, and authenticates and establishes an IP connection in the usual way.

5 The Foreign Agent informs the Home Agent that the Mobile Client is connected, and requests a tunnel. The Foreign Agent sends up to ten RegisterRequest messages at two-second intervals, timing out and logging a message if it receives no response to the requests.

6 The Home Agent requests a password before it creates the tunnel.

7 The Foreign Agent returns an encrypted version of the Ascend-Home-Agent-Password found in the Mobile Client's RADIUS profile. This password must match the Home

Agent's Password parameter in the ATMP configuration in the Ethernet Profile, including the case.

8 The Home Agent returns a RegisterReply with a number that identifies the tunnel. If registration fails, the DSL Terminator logs a message and the Foreign Agent disconnects the Mobile Client. If registration succeeds, the DSL Terminator creates the tunnel between the Foreign Agent and the Home Agent.

9 When the Mobile Client disconnects from the Foreign Agent, the Foreign Agent sends a DeregisterRequest to the Home Agent to close the tunnel. The Foreign Agent sends its request up to ten times or until it receives a DeregisterReply. If the Foreign Agent receives packets for a Mobile Client whose connection has been terminated, the Foreign Agent silently discards the packets.

Setting the UDP port

By default, ATMP agents use UDP port 5150 to exchange control information while establishing a tunnel. If the Home Agent ATMP profile specifies a different UDP port number, all tunnel requests to that Home Agent must specify the same UDP port.

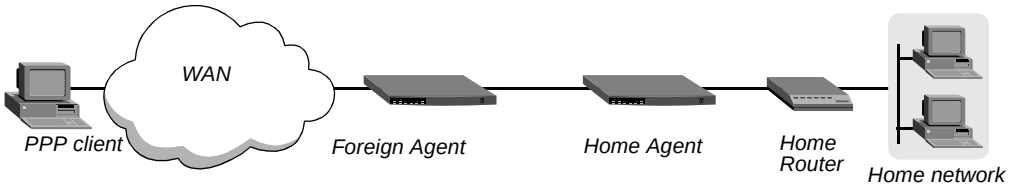
Note: A system reset is required for the ATMP subsystem to recognize the new UDP port number.

Setting an MTU limit

The type of link that connects a Foreign Agent and Home Agent determines the Maximum Transmission Unit (MTU). The link can be a Frame Relay connection or an Ethernet link, and it can be a local network or routed through multiple hops. If the link between devices is multihop (if it traverses more than one network segment), the path MTU is the *minimum* MTU of the intervening segments.

Figure 10-2 shows an ATMP setup across an Ethernet segment, which limits the path MTU to 1500 bytes.

Figure 10-2. Path MTU on an Ethernet segment



If any segment of the link between the agents has an MTU smaller than 1528, some packet fragmentation and reassembly occurs. You can push fragmentation and reassembly tasks to connection end points (a mobile client and a device on the Home network) by setting an MTU limit. The client software then uses MTU discovery mechanisms to determine the maximum packet size and fragments packets before sending them.

How link compression affects the MTU

Compression affects which packets must be fragmented because compressed packets are shorter than their original counterparts. If any kind of compression is on (such as VJ header or link compression), the connection can transfer larger packets without exceeding a link's

Maximum Receive Unit (MRU). If compressing a packet makes it smaller than the MRU, it can be sent across the connection, whereas the same packet without compression could not.

How ATMP tunneling causes fragmentation

To transmit packets through an ATMP tunnel, the DSL Terminator adds an 8-byte GRE header and a 20-byte IP header to the frames it receives. The addition of these packet headers can make the packet larger than the MTU of the tunneled link, in which case the DSL Terminator must either fragment the packet after encapsulating it or reject the packet.

Fragmenting packets after encapsulating them has several disadvantages for the Foreign Agent and Home Agent. Use of fragmentation causes a performance degradation because both agents have extra overhead. It also means that the Home Agent device cannot be a GRF switch. (To maintain its very high aggregate throughput, a GRF switch does not perform reassembly.)

Pushing the fragmentation task to connection end points

To avoid the extra overhead incurred when ATMP agents perform fragmentation, you can either set up a link between the two units that has an MTU greater than 1528 (which means it cannot include Ethernet segments), or you can set the Ethernet > Mod Config > ATMP > GRE MTU parameter to a value that is 28 bytes less than the path MTU.

If you set GRE MTU to zero (the default), the DSL Terminator might fragment encapsulated packets before transmission. The other ATMP agent must then reassemble the packets.

If you set GRE MTU to a nonzero value, the DSL Terminator reports that value to the client software as the path MTU, causing the client to send packets of the specified size. This pushes the task of fragmentation and reassembly out to the connection end points, lowering the overhead on the ATMP agents.

For example, if the DSL Terminator is communicating with another ATMP agent across an Ethernet segment, you can set the GRE MTU parameter to a value 28 bytes smaller than 1500 bytes, as shown in the following example, to enable the unit to send full-size packets that include the 8-byte GRE header and a 20-byte IP header without fragmenting the packets first:

```
GRE MTU = 1472
```

With this setting, the connection end point sends packets with a maximum size of 1472 bytes. When the DSL Terminator encapsulates them, adding 28 bytes to the size, the packets still do not violate the 1500-byte Ethernet MTU.

Forcing fragmentation for interoperation with outdated clients

To discover the path MTU, some clients normally send packets that are larger than the negotiated Maximum Receive Unit (MRU) and that have the Don’t Fragment (DF) bit set. Such packets are returned to the client with an ICMP message informing the client that the host is unreachable without fragmentation. This standard, expected behavior improves end-to-end performance by enabling the connection end points to perform any required fragmentation and reassembly.

However, some outdated client software does not handle this process correctly and continues to send packets that are larger than the specified GRE MTU. To enable the DSL Terminator to interoperate with such clients, configure the DSL Terminator to ignore the DF bit and perform

the fragmentation that is normally performed by the client software. This function in the DSL Terminator is sometimes referred to as *prefragmentation.*

When you set the GRE MTU parameter to a nonzero value, set the Force Fragmentation parameter to Yes to enable the DSL Terminator to prefragment packets it receives that are larger than the negotiated MRU with the DF bit set. It prefragments those packets, and then adds the GRE and IP headers.

Note: Setting the Force fragmentation parameter to Yes causes the DSL Terminator to bypass the standard MTU discovery mechanism and fragment larger packets before encapsulating them in GRE. Because this changes expected behavior, it is not recommended except for ATMP interoperation with outdated client software that does not handle fragmentation properly.

Router and gateway mode

A Home Agent can communicate with the Home network through a direct connection, through another router, or across a nailed connection. When the Home Agent relies on packet routing to reach the Home network, it operates in router mode. When it has a nailed connection to the Home network, it is in gateway mode.

Overview of RADIUS attributes for ATMP

The Foreign Agent must have a RADIUS user profile that authenticates the Mobile Client and specifies the attributes listed Table 10-1.

Table 10-1.RADIUS attributes required for ATMP connections

Attribute	Description	Possible values
Ascend-Home-Agent-Password (184)	Specifies the password that the Foreign Agent sends to the Home Agent during ATMP operation. This password must match the Home Agent's ATMP password.	Text string containing up to 20 characters. The default value is null.
Ascend-Home-Agent-UDP-Port (186)	Specifies the UDP port number for communicating ATMP messages between the Foreign Agent and the Home Agent.	Integer between 0 and 65535. The default value is 5150. You need not specify a value for Ascend-Home-Agent-UDP-Port if you specify a UDP port number for Ascend-Primary-Home-Agent or Ascend-Secondary-Home-Agent, or if you accept the default for either of these attributes.

Table 10-1.RADIUS attributes required for ATMP connections (continued)

Attribute	Description	Possible values
Ascend-Home-Network-Name (185)	Specifies the name of the Home Agent's nailed-up Connection profile to the Home network (required only if the Home Agent is operating in Gateway mode).	Text string. The default value is null.
Ascend-Primary-Home-Agent (129)	Specifies the first Home Agent the Foreign Agent tries to reach when setting up an ATMP tunnel, and indicates the UDP port the Foreign Agent uses for the link.	A symbolic hostname, or an IP address in dotted-decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. You can also specify an optional UDP port number. The default IP address is 0.0.0.0. The default UDP port number is 5150. **Note:** You can use Ascend-Home-Agent-IP-Addr in the user profile for the same purpose as Ascend-Primary-Home-Agent, but Lucent recommends the use of the Ascend-Primary-Home-Agent and Ascend-Secondary-Home-Agent to provide additional information in the user profile.
Ascend-Secondary-Home-Agent (130)	Specifies the secondary Home Agent which the Foreign Agent tries to reach when the primary Home Agent (specified by Ascend-Primary-Home-Agent) is unavailable. Also indicates the UDP port that the Foreign Agent uses for the link.	A symbolic hostname or an IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. You can also specify an optional UDP port number. The default IP address is 0.0.0.0. The default UDP port number is 5150.

Configuring a Foreign Agent

Following are the parameters (shown with sample settings) related to Foreign Agent configuration:

```
Ethernet
   Mod Config
      ATMP options...
         ATMP Mode=Foreign
         Type=N/A
         Password=N/A
```

```
            SAP Reply=N/A
            UDP Port=5150
            GRE MTU=1472
            Force fragmentation=No
            Idle limit=N/A
            ATMP SNMP Traps=No
```

Following are the parameters (shown with sample settings) for the IP routing connection to the Home Agent:

```
Ethernet
   Mod Config
      Ether options...
         IP Adrs=10.65.212.226/24

Ethernet
   Connections
    any Connection profile
      Station=name-of-home-agent
      Active=Yes
      Dial #=555-1212
      Route IP=Yes
      IP options...
         LAN Adrs=10.1.2.3/24
```

Following are the parameters (shown with sample settings) for using RADIUS authentication:

```
Ethernet
   Mod Config
      Auth...
         Auth=RADIUS
         Auth Host #1=10.23.45.11/24
         Auth Host #2=0.0.0.0/0
         Auth Host #3=0.0.0.0/0
         Auth Port=1645
         Auth Timeout=1
         Auth Key-=[]
         Auth Pool=No
         Auth Req=Yes
         Password Server=No
         Password Port=N/A
         Local Profile First=No
         Sess Timer=0
         Auth Src Port=0
         Auth Send Attr 6,7=Yes
```

Following are the parameters (shown with sample settings) for creating RADIUS user profiles for Mobile Clients running TCP/IP:

```
node1 Password="top-secret"
   Ascend-Metric=2,
   Framed-Protocol=PPP,
   Ascend-IP-Route=Route-IP-Yes,
   Framed-Address=200.1.1.2,
   Framed-Netmask=255.255.255.0,
   Ascend-Primary-Home-Agent=10.1.2.3,
   Ascend-Home-Agent-Password="private"
   Ascend-Home-Agent-UDP-Port = 5150
```

Understanding the Foreign Agent parameters and attributes

This section provides some background information about configuring a Foreign Agent to initiate an ATMP request to the Home Agent DSL Terminator. For detailed information about each parameter, see the *DSL Terminator Reference.* For details about attributes and configuring external authentication, see the *TAOS RADIUS Guide and Reference*.

Parameter(s)	**Usage**
ATMP Mode	Set this parameter to Foreign on the Foreign Agent. With the Foreign setting, the Type, and Password parameters do not apply.
UDP port	ATMP uses UDP port 5150 for ATMP messages between the Foreign Agent and Home Agent. If you specify a different UDP port number, make sure that the entire ATMP configuration uses the same port number.
GRE MTU	Specifies the Maximum Transmission Unit (MTU) for the path between the Foreign and Home Agents described in "Setting an MTU limit" on page 10-3.
ATMP SNMP Traps	Specifies that the DSL Terminator sends ATMP-related SNMP traps.
IP configuration and Connection profile parameters	The cross-Internet connection to the Home Agent is an IP routing connection that the DSL Terminator authenticates and establishes in the usual way. (For details, see Chapter 6, "Configuring IP Routing.")
RADIUS authentication attributes	The Foreign Agent must use RADIUS to authenticate Mobile Clients, and the RADIUS server must be running a version of the daemon that includes the ATMP attributes. (For details, see the *TAOS RADIUS Guide and Reference*.)
RADIUS user-profile attributes	The RADIUS user profiles for Mobile Clients must set ATMP attributes. The required attributes differ slightly, depending on whether the Mobile Client and Home network run IP and whether the Home Agent DSL Terminator operates in router mode or gateway mode.

Table 10-2 lists the required attributes when the Mobile Client and Home network are routing IP.

Table 10-2. Required RADIUS attributes to reach an IP Home network

Home Agent in router mode	**Home Agent in gateway mode**
`Ascend-Primary-Home-Agent`	`Ascend-Primary-Home-Agent`
`Ascend-Home-Agent-Password`	`Ascend-Home-Agent-Password`
`Ascend-Home-Agent-UDP-Port`	`Ascend-Home-Agent-UDP-Port`
	`Ascend-Home-Network-Name`

Following is a description of each Foreign Agent attribute:

Attribute	Description
`Ascend-Primary-Home-Agent`	IP address of the Home Agent, used to locate the Connection profile (or RADIUS profile) for the IP connection to the Home Agent.
`Ascend-Home-Agent-Password`	Used to authenticate the ATMP tunnel itself. Must match the password specified in the Home Agent's Ethernet > Mod Config > ATMP Options subprofile. All Mobile Clients use the *same* ATMP-Home-Agent-Password.
`Ascend-Home-Agent-UDP-Port`	Must match the UDP port configuration in Ethernet > Mod Config > ATMP Options. Required only for a port number other than the default 5150.
`Ascend-Home-Network-Name`	Name of the Home Agent's local Connection profile to the Home network. Required only when the Home Agent is operating in gateway mode (when it has a nailed WAN link to the Home network). For details, see "Configuring a Home Agent in gateway mode" on page 10-14.

Example of configuring a Foreign Agent (IP)

To configure the Foreign Agent and create a Mobile Client profile to access an IP Home network:

1 Open Ethernet > Mod Config > Ether Options and verify that the LAN interface has an IP address. For example:

```
Ethernet
   Mod Config
      Ether options...
         IP Adrs=10.65.212.226/24
```

2 Open the ATMP Options subprofile and set ATMP Mode to Foreign:

```
      ATMP options...
         ATMP Mode=Foreign
         Type=N/A
         Password=N/A
         SAP Reply=N/A
         UDP Port=5150
```

3 Open the Auth subprofile and configure the Foreign Agent to authenticate through RADIUS. For example:

```
      Auth...
         Auth=RADIUS
         Auth Host #1=10.23.45.11/24
         Auth Host #2=0.0.0.0/0
         Auth Host #3=0.0.0.0/0
         Auth Port=1645
         Auth Timeout=1
         Auth Key-=[]
         Auth Pool=No
```

```
Auth Req=Yes
Password Server=No
Password Port=N/A
Local Profile First=No
Sess Timer=0
Auth Src Port=0
Auth Send Attr 6,7=Yes
```

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

4 Close the Ethernet profile.

5 Open a Connection profile and configure an IP routing connection to the Home Agent. For example:

```
Ethernet
   Connections
     any Connection profile
      Station=home-agent
      Active=Yes
      Encaps=MPP
      Dial #=555-1212
      Route IP=Yes

      Encaps options...
         Send Auth=CHAP
         Recv PW=home-pw
         Send PW=foreign-pw

      IP options...
         LAN Adrs=10.1.2.3/24
```

6 Close the Connection profile.

7 On the RADIUS server, open the RADIUS user profile and create an entry for a Mobile Client. For example:

```
node1 Password="top-secret"
   Ascend-Metric=2,
   Framed-Protocol=PPP,
   Ascend-IP-Route=Route-IP-Yes,
   Framed-Address=200.1.1.2,
   Framed-Netmask=255.255.255.0,
   Ascend-Primary-Home-Agent=10.1.2.3,
   Ascend-Home-Agent-Password="private"
   Ascend-Home-Agent-UDP-Port = 5150
```

8 Close the user profile.

When the Mobile Client logs into the Foreign Agent with the password *top secret*, the Foreign Agent uses RADIUS to authenticate the Mobile Client. It then looks for a profile with an IP address that matches the Ascend-Home-Agent-IP-Addr value, so that it can bring up an IP connection to the Home Agent.

Configuring a Home Agent

To configure an ATMP Home Agent, set parameters in the ATMP profile, verify that the Home Agent can communicate across an IP link with the Foreign Agent, and configure the connection to the Home network.

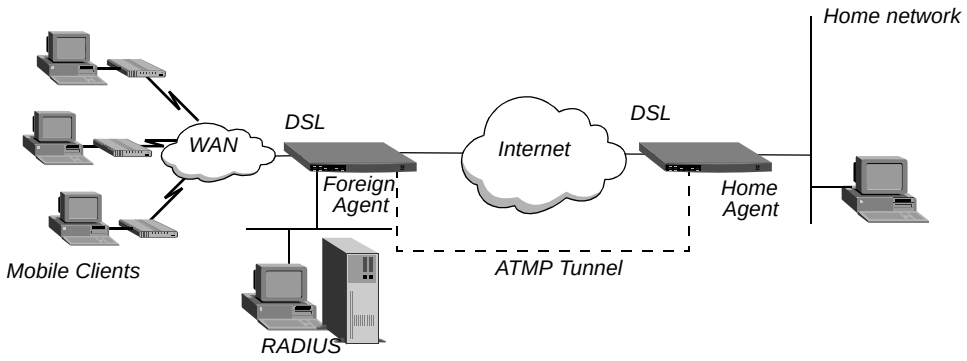
The link to the Foreign Agent can be any kind of connection (for example, nailed or Frame Relay) or an Ethernet link, and it can be a local network or a remote network provided the two units communicate through an IP network.

Because the Home Agent does not establish a connection on the basis of receiving tunneled data, the link to the Home network must be a nailed connection, a switched *incoming* connection from the Home network, or a routed connection.

Configuring a Home Agent in router mode

When the ATMP tunnel has been established between the Home Agent and Foreign Agent, the Home Agent in router mode receives IP packets through the tunnel, removes the GRE encapsulation, and passes the packets to its bridge or router software. In its routing table, the Home Agent adds a host route to the Mobile Client. Figure 10-3 shows an example of a a Home Agent in router mode.

Figure 10-3. Home Agent routing to the Home network



The following parameters (shown with sample settings) are used to configure a Home Agent in router mode:

```
Ethernet
   Mod Config
      Ether options…
         IP Adrs=10.1.2.3/24

      ATMP options...
         ATMP Mode=Home
         Type=Router
         Password=private
         SAP Reply=N/A
         UDP Port=5150
         GRE MTU=1472
         Force fragmentation=No
         Idle limit=0
         ATMP SNMP Traps=No
```

The IP routing connection *to* the Foreign Agent uses the following parameters (shown with sample settings):

```
Ethernet
   Connections
```

```
any Connection profile
  Station=foreign-agent
  Active=Yes
  Encaps=MPP
  Dial #=555-1213
  Route IP=Yes

  Encaps options...
     Send Auth=CHAP
     Recv PW=foreign-pw
     Send PW=home-pw

  IP options...
     LAN Adrs=10.65.212.226/24
```

Understanding the ATMP router mode parameters

This section provides some background information about configuring a Home Agent in router mode. For detailed information about each parameter, see the *DSL Terminator Reference.*

Parameter	**Usage**
ATMP Mode	For the Home Agent, the setting is Home.
Type	With the ATMP Type parameter set to Router, the Home Agent relies on routing (not a WAN connection) to pass packets received through the tunnel to the Home network.
Password	Password used to authenticate the ATMP tunnel itself. Must match the password specified in the Ascend-Home-Agent-Password attribute of each Mobile Client's RADIUS profile. (All Mobile Clients use the same password for that attribute.)
UDP Port	ATMP uses UDP port 5150 for ATMP messages between the Foreign Agent and the Home Agent. If you specify a different UDP port number, make sure that the entire ATMP configuration agrees.
Idle Limit	Specifies the number of minutes the Home Agent maintains an idle tunnel before disconnecting it.
GRE MTU	Specifies the Maximum Transmission Unit (MTU) for the path between the Foreign Agent and Home Agent as described in "Setting an MTU limit" on page 10-3.
Force fragmentation	Enable/disable prefragmentation of packets that have the DF bit set, as described in "Forcing fragmentation for interoperation with outdated clients" on page 10-4.
IP configuration and Connection profile parameters	The cross-Internet connection to the Foreign Agent is an IP routing connection that the DSL Terminator authenticates and establishes in the usual way. (For details, see the documentation that came with your unit.)

Routing to the Mobile Client

When the Home Agent receives IP packets through the ATMP tunnel, it adds a host route for the Mobile Client to its IP routing table. It then handles routing in the usual way.

For IP routes, you can enable RIP on the Home Agent's Ethernet to enable other hosts and networks to route to the Mobile Client. Enabling RIP is particularly useful if the Home

network is one or more hops away from the Home Agent's Ethernet. If you turn RIP off, other routers require static routes that specify the Home Agent as the route to the Mobile Client.

Note: If the Home Agent's Ethernet is the Home network (a direct connection), you should turn on proxy ARP in the Home Agent so that local hosts can use ARP to find the Mobile Client.

For details on IP routes, see the documentation that came with your unit.

Configuring a Home Agent in router mode (IP)

To configure the Home Agent in router mode to reach an IP Home network, proceed as follows:

1 Open Ethernet > Mod Config > Ether Options and verify that the LAN interface has an IP address. You can also set routing options. For example:

```
Ethernet
   Mod Config
      Ether options...
         IP Adrs=10.1.2.3/24
         RIP=On
```

2 Open the ATMP Options subprofile, set the ATMP Mode parameter to Home, and set the Type parameter to Router.

3 Specify the password used to authenticate the tunnel (Ascend-Home-Agent-Password). For example:

```
      ATMP options...
         ATMP Mode=Home
         Type=Router
         Password=private
         SAP Reply=N/A
         UDP Port=5150
         GRE MTU=1472
         Force fragmentation=No
         Idle limit=0
         ATMP SNMP Traps=No
```

4 Close the Ethernet profile.

5 Open a Connection profile and configure an IP routing connection *to* the Foreign Agent. For example:

```
Ethernet
   Connections
    any Connection profile
      Station=foreign-agent
      Active=Yes
      Encaps=MPP
      Dial #=555-1213
      Route IP=Yes

      Encaps options...
         Send Auth=CHAP
         Recv PW=foreign-pw
         Send PW=home-pw
```

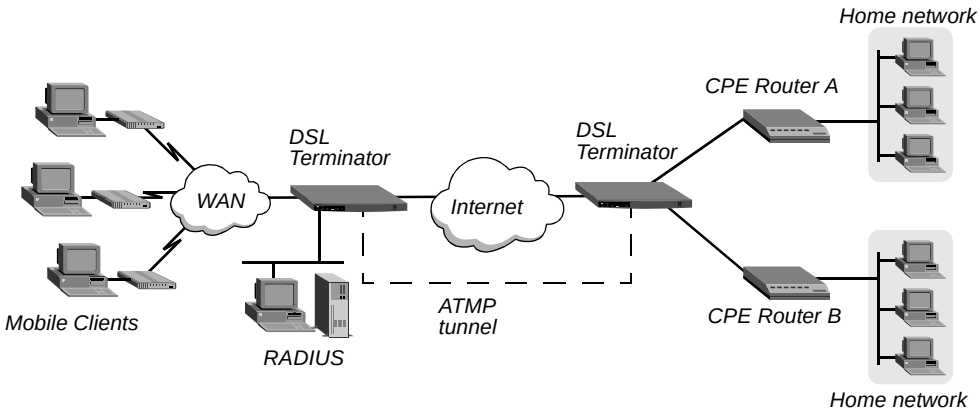
```
IP options...
   LAN Adrs=10.65.212.226/24
```

6 Close the Connection profile.

Configuring a Home Agent in gateway mode

When the ATMP tunnel has been established between the Home Agent and Foreign Agent, the Home Agent in router mode receives IP packets through the tunnel, removes the GRE encapsulation, and passes the packets to its bridge/router software. In its routing table, the Home Agent adds a host route to the mobile client. Figure 10-4 shows an example of Home Agent used in gateway mode. Figure 10-4 shows a Home Agent configured in gateway mode.

Figure 10-4. Home Agent in gateway mode



Note: To enable hosts and routers on the Home network to reach the Mobile Client, you must configure a static route in the Customer Premise Equipment (CPE) router on the Home network (not in the Home Agent). The static route must specify the Home Agent as the route to the Mobile Client. That is, the route's destination address specifies the Framed-Address of the Mobile Client, and its gateway address specifies the IP address of the Home Agent.

Limiting the maximum number of tunnels

If you decide to limit the maximum number of tunnels that a gateway will support, you should consider the expected traffic per mobile client connection, the bandwidth of the connection to the Home network, and the availability of alternative Home Agents (if any). For example, the lower the amount of traffic generated by each mobile client connection, the more tunnels a gateway connection will be able to handle.

Enabling RIP on the interface to the home router

The router at the far end of the gateway profile must be able to route back to mobile clients. The easiest way to accomplish this is to set the ATMP RIP parameter to Send-v2. With this setting, the gateway Home Agent constructs a RIP-v2 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 = 0.0.0.0, and metric = 1. RIP-v2 authentication and route tags are not supported.

Note: The Home network router must not send RIP updates, because the Home Agent does not inspect them. The RIP updates are forwarded to the mobile clients instead.

If you set ATMP RIP to Off, the administrator of the Home network must configure a static route to each mobile client. A static route to a mobile client can be specific to the client, where the route's destination is the mobile client IP address and the next-hop router is the Home Agent address. For example, in the following route the mobile client is a router (not a host route), and the Home Agent address is 2.2.2.2:

```
Dest=110.1.1.10/29
Gateway=2.2.2.2
```

Or, if the mobile clients have addresses allocated from the same address block (including router mobile client addresses with subnet masks less than 32 bits) and no addresses from that block are assigned to other hosts, the Home network administrator can specify a single static route that encompass all mobile clients that use the same Home Agent. For example, in the following route all mobile clients are allocated addresses from the 10.4.*n.n* block, and the Home Agent address is 2.2.2.2. No other hosts are allocated addresses from the 10.4.*n.n* block.

```
Dest=10.4.0.0/16
Gateway = 2.2.2.2
```

Configuring a Home Agent in gateway mode involves the following parameters (shown with sample settings):

```
Ethernet
   Mod Config
      Ether options…
         IP Adrs=10.1.2.3/24


      ATMP options...
         ATMP Mode=Home
         Type=Gateway
         Password=private
         SAP Reply=N/A
         UDP Port=5150
         GRE MTU=1472
         Force fragmentation=No
         Idle limit=0
         ATMP SNMP Traps=No
```

The IP routing connection to the Foreign Agent uses the following parameters (shown with sample settings):

```
Ethernet
   Connections
    any Connection profile
      Station=foreign-agent
      Active=Yes
      Encaps=MPP
      Dial #=555-1213
      Route IP=Yes
```

```
      Encaps options...
         Send Auth=CHAP
         Recv PW=foreign-pw
         Send PW=home-pw

      IP options...
         LAN Adrs=10.65.212.226/24
```

The nailed connection to the Home network uses the following parameters (shown with sample settings):

```
Ethernet
   Connections
      Station=homenet
      Active=Yes
      Encaps=MPP
      Dial #=N/A
      Calling #=N/A
      Route IP=Yes
     Route IPX=N/A

      IP options...
         LAN Adrs=5.9.8.2/24

      Telco options...
         Call Type=Nailed
         Group=1,2

      Session options...
         ATMP Gateway=Yes
         DSL Terminator ATMP Tunnels=0
         ATMP RIP=Send-v2
```

Understanding the ATMP gateway mode parameters

This section provides some background information about configuring a Home Agent in gateway mode. For detailed information about each parameter, see the *DSL Terminator Reference*.

Set the following parameters in the Mod Config profile's ATMP Options subprofile:

Parameter	**Usage**
ATMP Mode	For the Home Agent, the setting is Home.
Type	With the Type parameter set to Gateway, the Home Agent forwards packets received through the tunnel to the Home network across a nailed WAN connection.
Password	Authenticates the ATMP tunnel itself. Must match the password specified in the Ascend-Home-Agent-Password attribute of each Mobile Client's RADIUS profile. (All Mobile Clients use the same password for that attribute.)
UDP Port	ATMP uses UDP port 5150 for ATMP messages between the Foreign Agent and the Home Agent. If you specify a different UDP port number, make sure that the entire ATMP configuration agrees.
Idle limit	Specifies the number of minutes the Home Agent maintains an idle tunnel before disconnecting it.

Parameter	Usage
GRE MTU	Specifies the Maximum Transmission Unit (MTU) for the path between the Foreign Agent and the Home Agent as described in "Setting an MTU limit" on page 10-3.
Force fragmentation	Enables or disables prefragmentation of packets that have the DF bit set, as described in "Forcing fragmentation for interoperation with outdated clients" on page 10-4.

IP configuration and Connection profile

The cross-Internet connection to the Foreign Agent is an IP routing connection that the DSL Terminator authenticates and establishes in the usual way. For details, see the documentation that came with your unit.

Connection profile to the Home network

The Connection profile to the Home network must be a local profile. It cannot be specified in RADIUS. The name of this Connection profile must match the name specified by the Ascend-Home-Network-Name attribute in the Mobile Client's RADIUS profile. In addition, the Connection profile for connection to the Home network must specify the following values:

- Nailed call type. The Home Agent must have a nailed connection to the Home network, because it dials the WAN connection on the basis of packets received through the tunnel.
- ATMP Gateway session option enabled. The ATMP Gateway parameter must be set to Yes. This parameter instructs the Home Agent to send to the Mobile Client the data that it receives back from the Home network on this connection.
- ATMP tunnel limit. The DSL Terminator ATMP Tunnels parameter specifies the number of ATMP tunnels that the DSL Terminator as a Home Agent gateway can establish to a Home network. The maximum number of ATMP tunnels can be specified individually for each Home network.

You can also specify that the DSL Terminator include mobile-client routes in RIP-v2 responses to the home router. The ATMP RIP parameter specifies whether or not the DSL Terminator includes mobile-client routes in RIP-v2 responses to the home router.

Configuring a Home Agent in gateway mode (IP)

To configure the Home Agent in gateway mode to reach an IP Home network, proceed as follows:

1 Open Ethernet > Mod Config > Ether Options and verify that the LAN interface has an IP address. For example:

```
Ethernet
   Mod Config
      Ether options...
         IP Adrs=10.1.2.3/24
```

2 Open the ATMP Options subprofile, set ATMP Mode to Home, and set Type to Gateway.

3 Specify the password used to authenticate the tunnel. It must match the Ascend-Home-Agent-Password attribute of each Mobile Client's RADIUS profile. For example:

```
   ATMP options...
      ATMP Mode=Home
      Type=Gateway
      Password=private
      SAP Reply=N/A
      UDP Port=5150
      GRE MTU=1472
      Force fragmentation=No
      Idle limit=0
      ATMP SNMP Traps=No
```

4 Close the Ethernet profile.

5 Open a Connection profile and configure an IP routing connection to the Foreign Agent. For example:

```
Ethernet
   Connections
     any Connection profile
      Station=foreign-agent
      Active=Yes
      Encaps=MPP
      Dial #=555-1213
      Route IP=Yes

      Encaps options...
         Send Auth=CHAP
         Recv PW=foreign-pw
         Send PW=home-pw

      IP options...
         LAN Adrs=10.65.212.226/24
```

6 Open a Connection profile and configure a nailed WAN link to the Home network. For example:

```
Ethernet
   Connections
     any Connection profile
      Station=homenet
      Active=Yes
      Encaps=MPP
      Dial #=N/A
      Calling #=N/A
      Route IP=Yes

      IP options...
         LAN Adrs=5.9.8.2/24

      Telco options...
         Call Type=Nailed
         Group=1,2

      Session options...
         ATMP Gateway=Yes
         MAX ATMP Tunnels=0
         ATMP RIP=Send-v2
```

7 Close the Connection profile.

Specifying the tunnel password

A Home Agent typically requests a password before establishing a tunnel. The Foreign Agent returns an encrypted version of the password found in the mobile client profile.

If the password sent by the Foreign Agent matches the Password value specified in the ATMP profile, the Home Agent returns a RegisterReply with a number that identifies the tunnel, and the mobile client's tunnel is established. If the password does not match, the Home Agent rejects the tunnel, and the Foreign Agent logs a message and disconnects the mobile client.

Setting an idle timer for unused tunnels

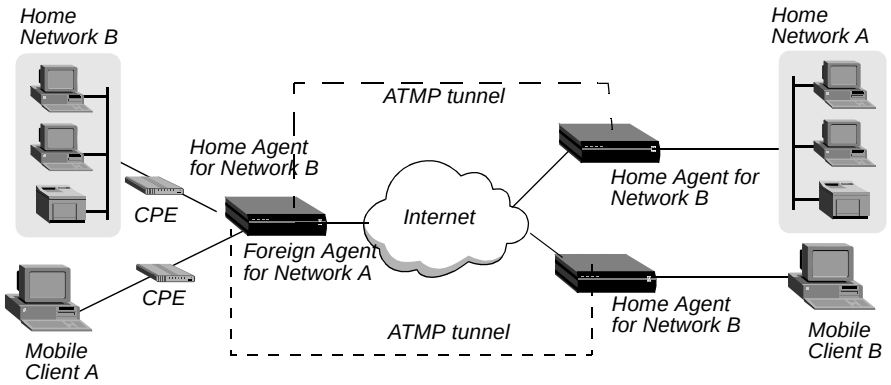
When a mobile client disconnects normally, the Foreign Agent sends a request to the Home Agent to close the tunnel. However, when a Foreign Agent restarts, tunnels that were established to a Home Agent are not normally cleared because the Home Agent is not informed that the mobile client is no longer connected. The unused tunnels continue to hold memory on the Home Agent. To enable the Home Agent to reclaim the memory held by unused tunnels, set an inactivity timer on a Home Agent by changing the Idle Limit parameter to a nonzero value.

The inactivity timer runs only on the Home Agent side and specifies the number of minutes (1 to 65535) that the Home Agent maintains an idle tunnel before disconnecting it. A value of 0 disables the timer, which means that idle tunnels remain connected forever. The setting affects only tunnels created after the timer was set. Tunnels that existed before the timer was set are not affected by the new setting.

Configuring the DSL Terminator as an ATMP multimode agent

You can configure the DSL Terminator to act as both a Home Agent and Foreign Agent on a tunnel-by-tunnel basis. Figure 10-5 shows a sample network topology that has a DSL Terminator acting as a Home Agent for Network B and a Foreign Agent for Network A.

Figure 10-5. DSL Terminator acting as both Home Agent and Foreign Agent



To configure the DSL Terminator as a multimode agent, set ATMP Mode to Both and complete both the foreign and Home Agent specifications. Setting ATMP Mode to Both indicates that the DSL Terminator will function as both a Home Agent and Foreign Agent on a tunnel-by-tunnel basis.

For example, to configure the DSL Terminator to operate as both a Home Agent and Foreign Agent, first check the interface and set the ATMP options:

1 Open Ethernet > Mod Config > Ether Options and verify that the LAN interface has an IP address. For example:

```
Ethernet
   Mod Config
      Ether options...
         IP Adrs=10.65.212.226/24
```

2 Open the ATMP Options subprofile and set ATMP Mode to Both.

3 Configure the other home-agent settings as appropriate. For example, to use Gateway mode and a password of *private*:

```
ATMP options...
   ATMP Mode=Both
   Type=Gateway
   Password=private
   SAP Reply=N/A
   UDP Port=5150
   GRE MTU=1472
   Force fragmentation=No
   Idle limit=0
   ATMP SNMP Traps=No
```

Then, set the Foreign Agent aspect of the multimode configuration:

1 Open the Auth subprofile and configure RADIUS authentication. For example:

```
Auth...
   Auth=RADIUS
   Auth Host #1=10.23.45.11/24
   Auth Host #2=0.0.0.0/0
   Auth Host #3=0.0.0.0/0
   Auth Port=1645
   Auth Timeout=1
   Auth Key-=[]
   Auth Pool=No
   Auth Req=Yes
   Password Server=No
   Password Port=N/A
   Local Profile First=No
   Sess Timer=0
   Auth Src Port=0
   Auth Send Attr 6,7=Yes
```

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

2 Close the Ethernet profile.

3 On the RADIUS server, open the RADIUS user profile and create an entry for a Mobile Client. For example:

```
node1 Password="top-secret"
   Ascend-Metric=2,
   Framed-Protocol=PPP,
   Ascend-IP-Route=Route-IP-Yes,
   Framed-Address=200.1.1.2,
   Framed-Netmask=255.255.255.0,
   Ascend-Primary-Home-Agent=10.1.2.3,
   Ascend-Home-Agent-Password="private",
```

```
   Ascend-Home-Agent-UDP-Port = 5150,
   Ascend-Home-Network-Name=home-agent
```

4 Close the user profile.

5 Open a Connection profile and configure an IP routing connection to the Network A Home Agent. For example:

```
Ethernet
   Connections
     any Connection profile
      Station=home-agent
      Active=Yes
      Encaps=MPP
      Dial #=555-1212
      Route IP=Yes

      Encaps options...
         Send Auth=CHAP
         Recv PW=home-pw
         Send PW=foreign-pw

      IP options...
         LAN Adrs=10.1.2.3/24
```

6 Close the Connection profile.

Finally, set the Home Agent parameters for multimode configuration:

1 Open a Connection profile and configure an IP routing connection to the Network B Foreign Agent. For example:

```
Ethernet
   Connections
    any Connection profile
      Station=foreign-agent
      Active=Yes
      Encaps=MPP
      Dial #=555-1213
      Route IP=Yes

      Encaps options...
         Send Auth=CHAP
         Recv PW=foreign-pw
         Send PW=home-pw

      IP options...
         LAN Adrs=10.65.212.226/24
```

2 Open a Connection profile and configure a nailed WAN link to the Network B Home network. For example:

```
Ethernet
   Connections
    any Connection profile
      Station=homenet
      Active=Yes
      Encaps=MPP
      Dial #=N/A
      Calling #=N/A
      Route IP=Yes

      IP options...
         LAN Adrs=5.9.8.2/24
```

```
Telco options...
   Call Type=Nailed
   Group=1,2

Session options...
   ATMP Gateway=Yes
   DSL Terminator ATMP Tunnels=0
   ATMP RIP=Send-v2
```

3 Close the Connection profile.

Supporting Mobile Client routers (IP only)

To enable an IP router to connect as a Mobile Client, the Foreign Agent's RADIUS entry for the Mobile Client must specify *the same subnet as the one that identifies the Home network*. For example, to connect to a Home network whose router has the address 10.1.2.3/28, the Foreign Agent's RADIUS entry for the remote router would contain lines such as the following:

```
node1 Password="top-secret"
   Ascend-Metric=2,
   Framed-Protocol=PPP,
   Ascend-IP-Route=Route-IP-Yes,
   Framed-Address=10.168.6.21,
   Framed-Netmask=255.255.255.240,
   Ascend-Primary-Home-Agent=10.1.2.3,
   Ascend-Home-Agent-Password="private"
```

With these Framed-Address and Framed-Netmask settings (equivalent to 10.168.6.21/28) for the Mobile Client router, the connecting LAN can support up to 14 hosts. The network address (or base address) for this subnet is 10.168.6.16. This address represents the network itself, because the host portion of the IP address is all zeros.

The broadcast address (all ones in host portion of address) for this subnet is 10.168.6.31. Therefore, the valid host address range is 10.168.6.17—10.168.6.30, which includes 14 host addresses.

The DSL Terminator handles routes to and from the Mobile Client's LAN differently, depending on whether the Home Agent is configured in router mode or gateway mode.

Home Agent in router mode

If the Home Agent connects directly to the Home network, set the Proxy ARP parameter to Always, which enables the Home Agent to respond to ARP requests on behalf of the Mobile Client. If the Home Agent does not directly connect to the Home network, the situation is the same as for any remote network: Routes to the Mobile Client's LAN must either be learned dynamically from a routing protocol or configured statically. The Mobile ClientMobile Client always requires static routes to the Home Agent as well as to other networks reached through the Home Agent. (It cannot learn routes from the Home Agent.)

Home Agent in gateway mode

If the Home Agent forwards packets from the Mobile Client across a nailed WAN link to the home IP network, the answering unit on the Home network must have a static route to the

Mobile Client's LAN. In addition, because no routing information passes through the connection between the Mobile Client and the Home Agent, the Mobile Client's LAN can support only local subnets that fall within the network specified in the RADIUS entry. For example, using the previous sample RADIUS entry, the Mobile Client can support two subnets with a mask of 255.255.255.248: one on the 10.168.6.16 subnet and the other on the 10.168.6.24 subnet. The answering unit on the Home network has only one route to the router itself (10.168.6.21/28).

ATMP connections that bypass a Foreign Agent

If a Home Agent DSL Terminator has the appropriate RADIUS entry for a Mobile Client, the Mobile Client connects directly to the Home Agent. An ATMP-based RADIUS entry that is local to the Home Agent enables the Mobile Client to bypass a Foreign Agent connection, but it does not preclude a Foreign Agent. If both the Home Agent and the Foreign Agent have local RADIUS entries for the Mobile Client, the node can choose a direct connection or a tunneled connection through the Foreign Agent.

Configuring PPTP tunnels

Point-to-Point Tunneling Protocol (PPTP) enables Microsoft Windows 95 and Windows NT Workstation users to connect to a local ISP and then to connect to a private corporate network across the Internet. To the user establishing the connection, the connection looks like a regular login to a Windows NT server that supports TCP/IP.

The DSL Terminator acts as a PPTP Access Controller (PAC) that functions as a front-end processor to offload the overhead of communications processing. At the other end of the tunnel, the NT server acts as a PPTP Network Server (PNS). All authentication is negotiated between the Windows 95 or NT client and the PNS. The Windows NT server's account information remains the same as if the client connected directly. No changes are needed.

How the DSL Terminator works as a PAC

You can configure a PPTP tunnel on a per-line or on a per-user basis. For a per-line tunnel, when a client connects to the DSL Terminator unit and wants to use a PPTP tunnel, the DSL Terminator unit chooses a tunnel on the basis of the Route Line *n* parameters. Each T1 PRI line is associated with a different Route Line *n* parameter. Each parameter specifies a particular PPTP server at the end of the PPTP tunnel. The DSL Terminator unit creates a tunnel for each T1 line on which the user connected.

In a RADIUS user profile, you specify the IP address or host name of a PPTP server. The profile creates a tunnel between the DSL Terminator unit and the PPTP server. When the name and password of an incoming call match the name and password in a RADIUS user profile set up for PPTP, the DSL Terminator unit creates the PPTP tunnel to the PPTP server.

The following section describes how to dedicate an entire WAN access line for each destination PNS address. For details about configuring WAN lines and assigning phone numbers, see the documentation that came with your unit.

In the PPTP configuration, you specify the destination IP address of the PNS (the Windows NT server), to which all calls that come in on the PPTP-routed line will be forwarded. When the DSL Terminator receives a call on that line, it passes the call directly to the specified IP

address end point, creating the PPTP tunnel to that address if one is not already up. The PNS destination IP address must be accessible by IP routing.

Note: The DSL Terminator handles PPTP sessions differently than it does regular sessions. No Connection profiles are used for these sessions, and the Answer profile is not consulted. The sessions are routed through the PPTP tunnel solely on the basis of the telephone number dialed.

Following are the PPTP PAC configuration parameters (shown with sample settings):

```
Ethernet
   Mod Config
      L2 Tunneling Options...
         PPTP Enabled=Yes
         Line 1 tunnel type=PPTP
         Route line 1=10.65.212.11
         Line 2 tunnel type=None
         Route line 2=0.0.0.0
         Line 3 tunnel type=None
         Route line 3=0.0.0.0
         Line 4 tunnel type=None
         Route line 4=0.0.0.0
```

Understanding the PPTP PAC parameters

This section provides some background information about configuring PPTP. For detailed information about each parameter, see the *DSL Terminator Reference*.

Enabling PPTP

When you enable PPTP, the DSL Terminator can bring up a PPTP tunnel with a 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.

Specifying a PRI line for PPTP calls and the PNS IP address

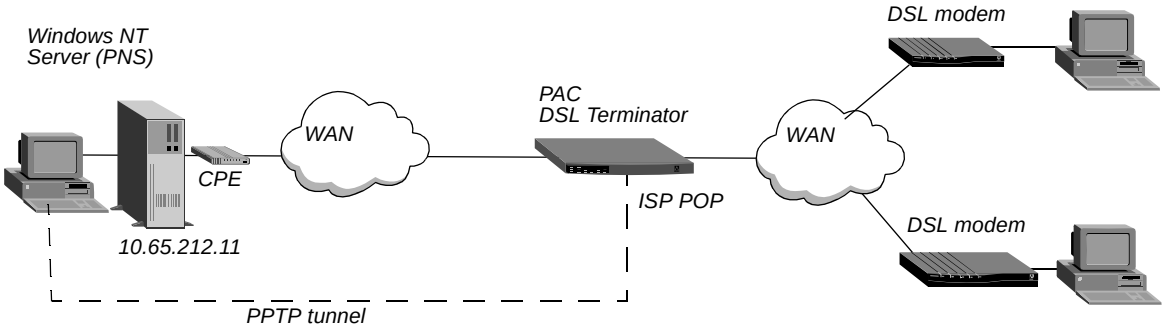
The PPTP parameters include four Route Line parameters, one for each of the DSL Terminator unit's WAN lines. If you specify the IP address of a PNS in one of these parameters, that WAN line is dedicated to receiving PPTP connections and forwarding them to that destination address.

The IP address you specify must be accessible via IP, but there are no other restrictions on it. It can be across the WAN or on the local network. If you leave the default null address, that WAN line handles calls normally.

Example of a PAC configuration

Figure 10-6 shows an ISP POP DSL Terminator unit communicating across the WAN with a Windows NT Server at a customer premise. Windows 95 or NT clients connect to the local ISP and are routed directly across the Internet to the corporate server. In this example, the DSL Terminator unit's fourth WAN line is dedicated to PPTP connections to that server.

Figure 10-6. PPTP tunnel



To configure this DSL Terminator for PPTP, proceed as follows:

1 Open Ethernet > Mod Config > PPTP Options.

2 Turn on PPTP, and set Route Line 4 to the PNS IP address.

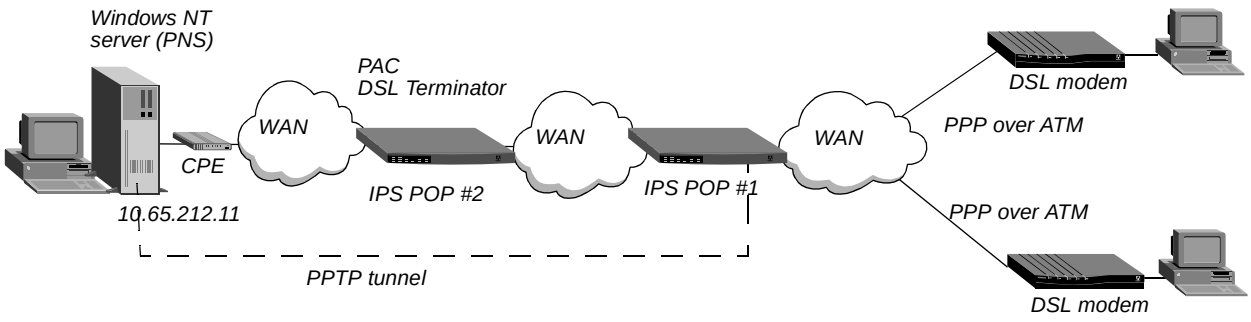
```
Ethernet
   Mod Config
      L2 Tunneling Options...
         PPTP Enabled=Yes
         Line 1 tunnel type=None
         Route line 1=0.0.0.0
         Line 2 tunnel type=None
         Route line 2=0.0.0.0
         Line 3 tunnel type=None
         Route line 3=0.0.0.0
         Line 4 tunnel type=PPTP
         Route line 4=10.65.212.11
```

3 Close the Ethernet Profile.

Example of a PPTP tunnel across multiple POPs

Figure 10-7 shows an ISP POP DSL Terminator communicating through an intervening router to the PNS that is the end point of its PPTP tunnel. The DSL Terminator routes the packets in the usual way to reach the end point IP address.

Figure 10-7. PPTP tunnel across multiple POPs



In this example, the DSL Terminator at ISP POP #1 dedicates its second WAN line to PPTP connections to the PNS at 10.65.212.11. To configure this DSL Terminator as a PAC, proceed as follows:

1 Open Ethernet > Mod Config > PPTP Options.

2 Turn on PPTP, and specify the PNS IP address for Route Line 2.

```
Ethernet
   Mod Config
      L2 Tunneling Options...
         PPTP Enabled=Yes
         Line 1 tunnel type=None
         Route line 1=0.0.0.0
         Line 2 tunnel type=PPTP
         Route line 2=10.65.212.11
         Line 3 tunnel type=None
         Route line 3=0.0.0.0
         Line 4 tunnel type=None
         Route line 4=0.0.0.0
```

3 Close the Ethernet Profile.

The PAC must have a route to the destination address, in this case a route through the ISP POP #2. It does not have to be a static route. It can be learned dynamically by means of routing protocols. The remaining steps of this procedure configure a static route to ISP POP #2:

4 Open an unused IP Route profile and activate it. For example:

```
Ethernet
   Static Rtes
      Name=pop2
      Active=Yes
```

5 Specify the PNS destination address:

```
Dest=10.65.212.11
```

6 Specify the address of the next-hop router (ISP POP #2). For example:

```
Gateway=10.1.2.4
```

7 Specify a metric for this route, the route's preference, and whether the route is private. For example:

```
Metric=1
Preference=100
Private=Yes
```

8 Close the IP Route profile.

Routing a terminal-server session to a PPTP server

You can initiate a PPTP session in which the terminal-server interface routes the session to a PPTP server. The PPTP command gives you two options for selecting the tunnel the DSL Terminator creates. You can specify either the IP address or host name of the PPTP server. Normal PPTP authentication proceeds once the DSL Terminator creates the tunnel.

Enter the command, at the terminal-server prompt as follows:

`pptp` *pptp_server*

where `pptp_server` is the IP address or hostname of the PPTP server. When you enter the command, the system displays the following text:

```
PPTP: Starting session

PPTP Server pptp_server
```

Configuring L2TP tunnels

L2TP enables you to connect to a local ISP and then to connect to a private corporate network across the Internet. You connect to a local L2TP Access Concentrator (LAC) and establish a PPP connection. Attributes in your RADIUS user profile specify that the DSL Terminator, acting as a LAC, establishes an L2TP tunnel. The LAC contacts the L2TP Network Server (LNS) that connects to the private network. The LAC and the LNS establish an L2TP tunnel (via UDP), and any traffic your client sends is tunneled to the private network. Once the DSL Terminator units establish the tunnel, the client connection has a PPP connection with the LNS, and appears to be directly connected to the private network.

You can configure the DSL Terminator to act as either a LAC, an LNS, or both. The LAC performs the following functions:

- Establishes PPP connections with remote clients.
- Sends requests to LNS units, requesting creation of tunnels.
- Encapsulates and forwards all traffic from clients to the LNS via the tunnel.
- De-encapsulates traffic received from an established tunnel and forwards it to the client.
- Sends tunnel-disconnect requests to LNS units when clients disconnect.

The LNS performs the following functions:

- Responds to requests by LAC units for creation of tunnels.
- Encapsulates and forwards all traffic from the private network to clients via the tunnel.
- De-encapsulates traffic received from an established tunnel, and forwards it to the private network.
- Disconnects tunnels on the basis of requests from the LAC.
- Disconnects tunnels when the value you set for a user profile's DSL Terminator-Connect-Time attribute expires. You can also manually disconnect tunnels from the LNS by using SNMP, the terminal-server Kill command, or the DO Hangup command (which you access by entering Ctrl- D).

Note: In the current software version, a DSL Terminator acting as an LNS cannot send Incoming Call Requests to a LAC. Only a LAC can make requests for the creation of L2TP tunnels.

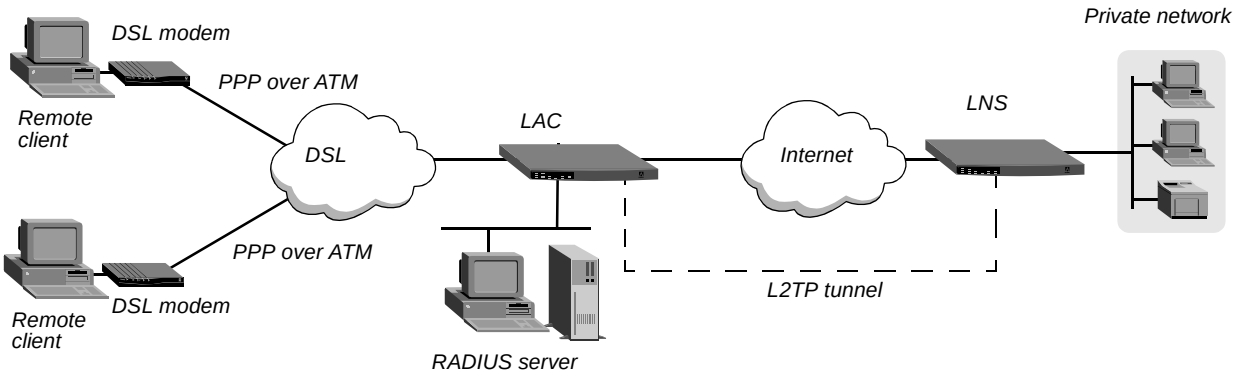
Elements of L2TP tunneling

This section describes how L2TP tunnels work between a LAC and an LNS. A client connects to a LAC, from either a modem or ISDN device, and the LAC establishes a cross-Internet IP connection to the LNS. The LAC then requests an L2TP tunnel via the IP connection.

The LNS is the terminating part of the tunnel, where most of the L2TP processing occurs. It communicates with the private network (the destination network for the remote clients) through a direct connection.

Figure 10-8 shows an ISP POP DSL Terminator, acting as a LAC, communicating across the WAN with a private network. Clients connect to the ISP POP and are forwarded across the Internet to the private network.

Figure 10-8. L2TP tunnel across the Internet



How the DSL Terminator creates L2TP tunnels

The remote client, the LAC, and the LNS establish, use, and terminate an L2TP-tunnel connection as follows:

1. A client connects, over either a DSL modem or a PPP over Ethernet connection, into the LAC.
2. After authentication (depending on the LAC configuration), the LAC communicates with the LNS to establish an IP connection.
3. Over the IP connection, the LAC and LNS establish a control channel.
4. The LAC sends an Inbound Call Request to the LNS.
5. Depending on the LNS configuration, the client might need to authenticate itself a second time.
6. After successful authentication, the tunnel is established, and data traffic flows.
7. When the client disconnects from the LAC, the LAC sends a Call Disconnect Notify message to the LNS. The LAC and LNS disconnect the tunnel.

LAC and LNS mode

The DSL Terminator unit can function as an LAC, an LNS, or both. L2TP supports multimode in which a unit is both a LAC (foreign agent) and a LNS (home agent). As L2TP LNS, the unit terminates the L2TP session and authenticates the user. If the user's profile on the LNS calls for an L2TP tunnel, the LNS then switches that user's session. The unit acts as an L2TP LAC and originates a new L2TP tunnel and session. The MAX unit operates as an LNS as far as the first LAC is concerned, and as an LAC as far as the next hop is concerned.

In L2TP switching, a MAX unit can be both a LNS and a LAC simultaneously for the same session. The session arrives and is serviced by the unit acting as a LNS.

Tunnel authentication

You can configure the LNS to authenticate a tunnel during tunnel creation. You must enable tunnel authentication on both the LAC and LNS.

On the LNS, you must create a Names/Passwords profile where:

- The value in the Ethernet > Names/Passwords > Name parameter matches the value of the System > Sys Config > Name parameter on the LAC.
- The value of the Ethernet > Names/Passwords > Recv PW parameter matches the password configured on the LAC.

On the LAC, you can specify the password with the Tunnel-Password attribute in the RADIUS user profile for the connection initiating the session, or you can configure the password in a Names/Passwords profile. If you create a Names/Passwords profile, the value of the Ethernet > Names/Passwords > Name parameter must match the value of the System > Sys Config > Name parameter on the LNS.

You can also configure the LAC and LNS to *not* require tunnel authentication.

Client authentication

Either the LAC, the LNS, or both, can perform PAP or CHAP authentication of clients for which they create tunnels. Because the DSL Terminator automatically builds a tunnel to the LNS for any call it receives on that line, if you configure the DSL Terminator to create tunnels on a per-line basis, only the LNS can perform authentication,.

If you use RADIUS to configure L2TP on a per-user basis, and you specify the Client-Port-DNIS attribute, the LAC does not perform PAP or CHAP authentication. If you specify Client-Port-DNIS, the tunnel is created as soon as the LAC receives a DNIS number that matches a Client-Port-DNIS for any user profile. You can configure the LNS to perform PAP or CHAP authentication after the LAC and LNS establish the tunnel.

If you use RADIUS to configure L2TP, but do not specify the Client-Port-DNIS attribute, the LAC performs PAP or CHAP authentication before the tunnel is established. Once the tunnel is up, the LNS can perform authentication again on the client. Each client sends the same username and password during the authentication phase, so for each client, make sure you configure the LAC and LNS to look for the same usernames and passwords.

You can also direct the DSL Terminator to create an L2TP tunnel, from the terminal server, by using the L2TP command. You can configure authentication on the LNS, requiring users to authenticate themselves when they manually initiate L2TP tunnels from the terminal server.

Flow control

The LAC and LNS automatically use a flow control mechanism that is designed to reduce network congestion. You do not need to configure the mechanism.

You can, however, configure the maximum number of unacknowledged packets that the LAC or LNS receives before it requests that the sending device stop sending data. You can configure the LAC or LNS to receive up to 63 unacknowledged packets before refusing new data, or you can disable flow control completely.

The LAC is responsible for requesting L2TP tunnels to the LNS. You configure the LAC to determine when a connection is tunneled, and you can specify the LNS used for the connection.

Understanding the L2TP LAC parameters

This section provides some background information about parameters used in configuring the DSL Terminator as a LAC:

Parameter	**Usage**
L2TP Mode	Enables the DSL Terminator unit's LAC functionality if you set L2TP Mode to LAC or Both.
L2TP Auth Enabled	Enable tunnel authentication for both the LAC and LNS or enable it for neither. You configure a tunnel password in a Names/Passwords profile.
L2TP RX Window	Specifies the number of unacknowledged packets the DSL Terminator receives (when configured as a LAC or an LNS) before requesting that the sending device stop transmitting data.
Line *N* Tunnel Type	Specifies whether the DSL Terminator should dedicate an entire WAN line to either L2TP or PPTP. If you want the DSL Terminator to establish tunnels on a connection-by-connection basis, set Line *N* Tunnel Type to None on all lines.
Route Line *N*	Specifies the IP address of the LNS. This parameter applies *only* if you dedicate an entire WAN line to tunneling with the Line *N* Tunnel Type parameter. If you want the DSL Terminator to establish tunnels on a connection-by-connection basis, leave Route Line *N* blank for all lines.

Configuring systemwide L2TP LAC parameters

To configure the DSL Terminator as an L2TP LAC, you must first enable L2TP LAC on the DSL Terminator, then specify how the DSL Terminator determines which connections are tunneled.

To configure systemwide L2TP LAC parameters on the DSL Terminator, proceed as follows:

1 Open the Ethernet > Mod Config > L2 Tunneling Options menu.

2 Set L2TP Mode to LAC or to Both.

3 If you require tunnel authentication, set L2TP Auth Enabled to Yes.

You must configure both the LAC and LNS identically, either to require or not require authentication.

4 Set L2TP RX Window to the number of packets that the DSL Terminator receives before it requests the sending device to stop transmitting packets.

The default is 7. Set the parameter to 0 (zero) to disable flow control in the receiving direction. The DSL Terminator continues to perform flow control for the sending direction regardless of the value of L2TP RX Window.

Enabling L2TP tunneling for an entire WAN line

If you want the LAC to create L2TP tunnels for every call received on a specific WAN line:

1 Open the Ethernet > Mod Config > L2 Tunneling Options menu.

2 For the line for which you are configuring LAC functionality (Line *N*), set Line *N* Tunnel Type to L2TP. For example, if you want to tunnel all calls received on the first WAN port (labeled WAN 1 on the DSL Terminator back panel), set Line 1 Tunnel Type to L2TP.

3 Set Route line *n* to the IP address of the LNS.\

Enabling L2TP tunneling on a per-user basis

You can configure RADIUS to direct the DSL Terminator to create L2TP tunnels for specific users. To do so, you use three standard RADIUS attributes: Tunnel-Type, Tunnel-Medium-Type, and Tunnel-Server-Endpoint. Table 10-3 describes them.

Table 10-3.RADIUS attributes for specifying L2TP tunnels

Attribute	Description	Possible values
Tunnel-Type (64)	Specifies which tunneling protocol to use for this connection.	PPTP or L2TP. You must set this attribute to L2TP to direct the DSL Terminator to create an L2TP tunnel.
Tunnel-Medium-Type (65)	Specifies the protocol type, or medium, used for this connection. Currently, the DSL Terminator supports IP only. Future software releases will support additional medium types.	Currently, the only supported value is IP. You must set this attribute to IP.
Tunnel-Server-Endpoint (67)	Specifies the IP address or fully qualified host name of the LNS, if you set Tunnel-Type to L2TP or PPTP Network Server (PNS), if you set Tunnel-Type to PPTP.	If a DNS server is available, you can specify the fully qualified hostname of the LNS. Otherwise, specify the IP address of the LNS in dotted decimal notation (*n.n.n.n*, where *n* is a number from 0 to 255.) You must set this attribute to an accessible IP host name or address.

If the LNS is on a remote IP network, the DSL Terminator unit requires a RADIUS profile (or comparable IP-routing Connection profile) to the LNS. For example:

```
l2tp-1 Password = "lac-pw"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Framed-Address = 1.1.1.1
```

```
route-tnt-1 Password = "ascend", User-Service = Dialout-Framed-User
    Framed-Route = "1.0.0.0 1.1.1.1 1 n l2tp-1-out"
l2tp-1-out Password = "lac-pw" User-Service = Dialout-Framed-User
    User-Name = "l2tp-1",
    Ascend-Dial-Number = "9-1-333-555-1212",
    Framed-Protocol = MPP,
    Framed-Address = 1.1.1.1,
    Ascend-Send-Password = "lns-pw"
```

Configuring the DSL Terminator as an LNS

When the DSL Terminator is configured as an LNS, it responds to requests by LAC units to establish tunnels. An LNS does not initiate outgoing requests for tunnels, so configuration of the DSL Terminator is simple. Proceed as follows:

1 Open the Ethernet > Mod Config > L2 Tunneling Options menu.

2 Set L2TP Mode to either LNS or Both.

3 If you require tunnel authentication, set L2TP Auth Enabled to Yes.

You must configure both the LAC and LNS identically, to either require or not require authentication.

4 Set L2TP RX Window to the number of packets that the DSL Terminator should receive before it requests that the sending device stop transmitting packets.

The default is 7. Set the parameter to 0 (zero) to disable flow control in the receiving direction. The DSL Terminator continues to perform flow control for the sending direction regardless of the value of L2TP RX Window.

Configuring L2TP Mobile Client profiles

When a DSL Terminator unit answers a PPP call, it initiates an L2TP tunnel to the LNS if the caller's profile is configured to do so. It can bring up a tunnel on the basis of the call's DNIS or CLID information, or it can password-authenticate the call and then initiate the tunnel.

L2TP settings in RADIUS profiles

RADIUS uses the following attribute-value pairs to specify L2TP tunnels:

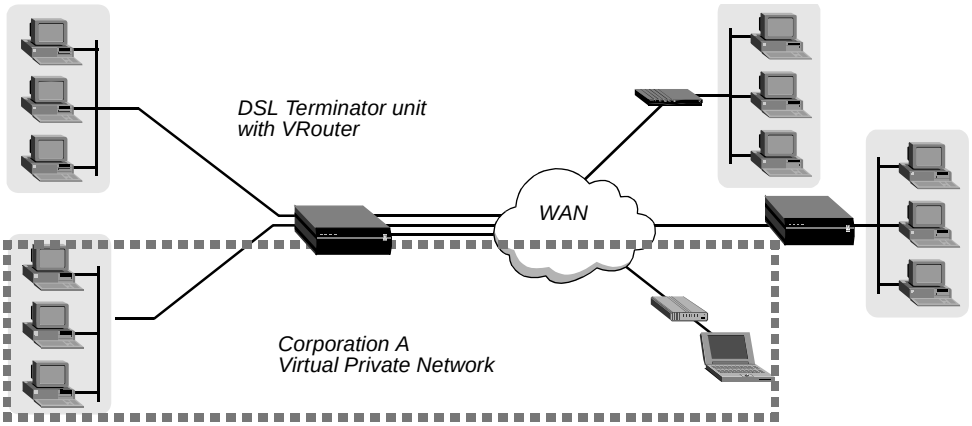
Attribute	**Value**
Tunnel-Type (64)	Tunneling protocol to be used. Set to L2TP (3) for L2TP tunneling.
Tunnel-Medium-Type (65)	Media to be used for the tunnel. Only IP (1) is supported at this time.
Tunnel-Server-Endpoint (66)	DNS hostname or dotted IP address of the LNS endpoint (a string value). If it specifies a hostname, the DSL Terminator unit executes a DNS lookup for the host's address.

Configuring Virtual Routers

A single DSL Terminator unit can support multiple, mutually exclusive routing tables called *Virtual Routers (VRouters)*. VRouters group routing interfaces in the DSL Terminator unit. Each VRouter has its own associated routing table, ARP table, route cache, address pools, and maintains its own routing and packet statistics.

If you do not configure any VRouters, the DSL Terminator unit's router operates as it has in earlier versions of the software. When you configure one or more VRouters, the main router operates as the global VRouter. All interfaces that are not explicitly grouped with a defined VRouter are grouped with the global VRouter.

Figure 10-9. Typical VRouter implementation



Before Lucent Technologies introduced VRouters, the DSL Terminator unit maintained a single IP routing table that enabled the router to reach any interface. In that context, each interface known to the system required a unique address.

With VRouters, addresses must be unique within the VRouter's routing domain, but not necessarily within the DSL Terminator unit. Because each VRouter maintains its own routing table, and because it knows only about those interfaces that explicitly specify the same VRouter, private networks do not maintain unique address spaces.

Current limitations

SNMP management does not present a view of the DSL Terminator on a per-VRouter basis. Errors and events are not logged on a per-VRouter basis. The Syslog host defined in the system's Log profile must be accessible to the main VRouter.

Only the main VRouter supports ATMP, PPTP, and OSPF.

The servers and clients you specify in the following profiles must be accessible to the main VRouter:

- Accounting
- Auth
- BOOTP Relay
- Call logging

- DHCP options
- Log
- Multicast
- RADIUS Server
- SNMP Options and SNMP Traps
- SNTP Server
- Stack Options
- TCP Modem Options
- TServ Options
- Trap

Creating a Virtual Router profile

All Virtual Routers parameters apply to only one Virtual Private Network (VPN). You can configure up to sixteen Virtual Router profiles. You must activate a Virtual Router profile for each VRouter. For example:

```
90-C00 Virtual Routers
90-C01 vr1
90-C02 -atmp-net
90-C02 -vr999
```

Each VRouter has its own routing protocol handler. For each VRouter, the DSL Terminator unit creates a new instance of the RIP protocol to process routes. The new instance of RIP sends and receives update packets only on the interfaces associated with its particular VRouter and manipulates only that VRouter's routing table. All RIP-related parameters in the Virtual Router profile use default settings that are recommended for most sites. The following sections outline the parameters that you must specify.

Required Virtual Routers profile settings

To enable VRouters, you must specify a name for the VRouter and specify that the VRouter profile is Active. To do this, you must set the Name parameter in the Virtual Routers profile.You must set the Active parameter, also in the Virtual Routers profile, to Yes. For example:

```
Name=vr1
Active=Yes
```

Required Connection profile settings

In the Connection profile's IP Options, you must set the Virtual Router parameter to the same name you set in the Virtual Routers profile. This refers to the DSL Terminator unit's Connection profile to the VRouter. For example:

```
Virtual Router=vr1
```

Required Static Rtes profile settings

To enable VRouters to use static routes, you must set the Virtual Router parameter in the Static Rtes profile to the same name you set in the Virtual Routers profile. For example:

```
Virtual Router=vr1
```

An *inter-VRouter* is created when you specify the name of a VRouter as the route's next hop. To enable inter-Vrouters, you must set the Dest parameter, the Dest VRouter parameter, and the Virtual Router parameter in the Static Rtes profile. In the same profile, you must also verify that the Gateway parameter's default setting, 0.0.0.0, is specified. The DSL Terminator unit sends packets destined for the destination address to the specified VRouter, which consults its own routing table to further route the packets. Set the Gateway-Address parameter the zero address, `0.0.0.0`, for this parameter to apply. For example:

```
Dest=10.207.23.1
Gateway=0.0.0.0
Virtual Router=vr1
Dest VRouter=vr2
```

In the previous example, the Dest parameter, specifies the destination IP address, 10.207.23.1. Specifying the name of another active virtual router, `vr2`, in the Dest VRouter parameter indicates that there is a static route between the VRouters. The Virtual Router parameter specifies the name of the VRouter for which the DSL Terminator unit creates the static route, the same name as the one specified in the Virtual Routers profile, `vr1`.

Disabling a Virtual Router profile

Disabling a Virtual Router profile disables the VRouter itself. For example:

```
Active=No
```

If you disable a VRouter with active connections, you must reset the DSL Terminator unit. If you cannot reset the unit, manually tear down any active connection, and then modify the local Connection and Static Rtes profiles that point to the VRouter. Specify that the local Connection and Static Rtes profiles to point to the global VRouter or another existing VRouter.

Understanding VRouter parameters

Existing parameters in the DNS profile are replicated in the Virtual Routers profile. The parameters in the DNS profile apply only to the global VRouter. The DSL Terminator unit's Ethernet port always connects to the global VRouter.

The following existing parameters support VRouters:

- Name
- Active
- Domain Name
- Dest
- Sec Domain Name
- Pri DNS
- Sec DNS

- Allow As Client DNS
- RIP Policy
- RIP Summary
- RIP Trigger
- Pool Summary
- Pool#n start
- Pool#n count
- Pool#n name

In addition, two new parameters support VRouter IP Adrs parameter appears in the Virtual Routers profile. The Virtual Router parameter appears in the Connections and Static Rtes profiles.

Parameter	Description
Dest VRouter	Specifies whether or not there is a static route between VRouters and, if there is, the name of the destination VRouter. Specify the name of the destination VRouter. You can specify the main VRouter as the destination.The default is 0.0.0.0, which specifies that this is not a static route between VRouters. The Dest VRouter setting is valid only if the Sys Option Status display specifies VRouter Avail.
Virtual Router	Specifies the name of the Virtual Router (VRouter) for which the DSL Terminator unit creates a Static Route. Specify the name of a Virtual Router. The default is null, which specifies that the unit uses the global Virtual Router (Main).
VRouter IP Adrs	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. Specify an IP address in dotted decimal notation. The default is 0.0.0.0.

RADIUS attributes

You can configure following vendor-specific attributes to configure VRouter settings on the DSL Terminator unit:

Attribute	Value
Ascend-IP-Pool-Definition (217)	Specifies the first IP address in an IP address pool, the number of addresses in the pool, and a Virtual Router (VRouter). If you do not indicate the name of a VRouter, the DSL Terminator unit uses the global VRouter, usually Main.

Attribute	Value
Ascend-Tunnel-VRouter-Name (31)	Specifies the VRouter that the DSL Terminator unit uses to establish a Layer 2 Tunnel Protocol (L2TP)or Layer 2 Forwarding (L2F) tunnel.
Ascend-VRouter-Name (102)	Specifies the name of a defined Virtual Router (VRouter). Specifying the VRouter name in a RADIUS user profile groups the WAN interfaces with the VRouter. Specify the name of a VRouter. The default is null, which specifies that the global VRouter is in use.
Framed-Route (22)	Specifies a static IP route, which is added to the DSL Terminator unit's routing table. Limit Each pseudo-user profile to about 25 routes (specify up to 25 settings for the Framed-Route attribute in a pseudo-user profile). The unit fetches information from each entry in order to initialize its routing table.

Defining Static Filters

11

Introduction to filters 11-1
Defining generic filters 11-6
Defining IP filters. 11-10
Defining Type of Service filters. 11-17
Applying a filter to an interface 11-22

Introduction to filters

A filter consists of specifications describing packets and actions to take upon packets that match the descriptions. After you apply a filter to an interface, the DSL Terminator unit monitors the data stream on that interface.

Depending on how you define a filter, it can apply to inbound packets, outbound packets, or both. In addition, filters are flexible enough to specify taking an action (such as forward or drop) on those packets that match the specifications, or on all packets *except* those that match the specifications.

Basic types of filters

Each Filter profile contains up to 12 input filters (applied to inbound packets) and 12 output filters (applied to outbound packets). Each of the up to 24 specifications can be one of the following basic types of filters:

- Generic filters
- IP filters
- Type of Service filters

Generic filters examine the byte- or bit-level contents of any packet, comparing specified or bits with a value defined in the filter. On the basis of this comparison, the filter specifies a forwarding action. They specify a forwarding action based on a comparison between certain bytes or bits in a packet and a value defined in the filter. To use generic filters effectively, you need to know the contents of certain bytes in the packets you wish to filter. Protocol specifications are usually the best source of such information.

IP filters apply only to IP-related packets. They specify a forwarding action on the basis of higher-level fields in IP packets (for example, the source or destination address, or the protocol number). They operate on logical information, which is relatively easy to obtain.

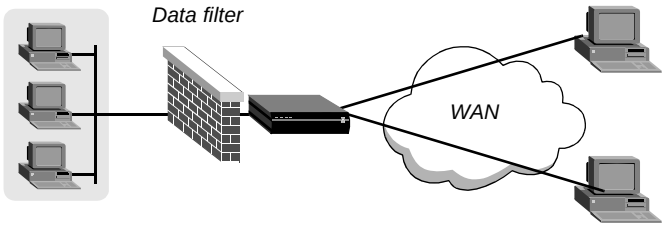
Type of Service (TOS) filters set priority bits in the TOS header of IP packets. Other routers can then use the information to prioritize and select links for particular data streams.

Data and call filters

Data filters are commonly used for security, but they can apply to any purpose that requires the DSL Terminator unit to drop or forward specific packets. The focus is typically on keeping out traffic that you do not want on a LAN. For example, you can use data filters to drop packets addressed to particular hosts or to prevent broadcasts from going across the WAN. You can also use data filters to allow users to access only specific devices across the WAN.

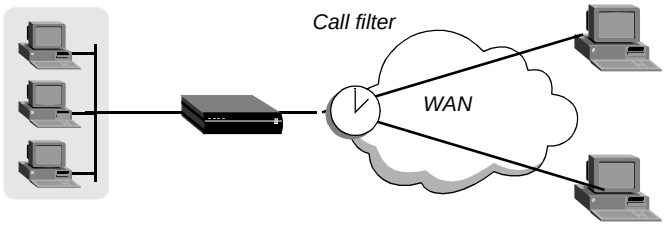
When you apply a data filter, its forwarding action (forward or drop) affects the actual data stream by preventing certain packets from reaching the Ethernet from the WAN, or vice versa. Data filters do not affect the idle timer, and a data filter applied to a Connection profile does not affect the answering process.

Figure 11-1. Data filters drop or forward certain packets



Call filters prevent unnecessary connections and help the DSL Terminator unit distinguish active traffic from *noise*. By default, any traffic to a remote site triggers a call, and any traffic across an active connection resets the connection's idle timer.

Figure 11-2. Call filters prevent certain packets from resetting the timer



When you apply a call filter, its forwarding action (forward or drop) does *not* affect which packets are sent across an active connection. The forwarding action of a call filter determines which packets can either initiate a connection or reset a session's timer. When a session's idle timer expires, the session is terminated. With the default Idle Timer setting of 120 seconds, the DSL Terminator unit terminates a connection that has been inactive for two minutes.

How filters work

A Filter profile can include up to 12 input-filter and 12 output-filter specifications (filters). Each filter has its own forwarding action—forward or drop. The filters are applied in sequence.

At the first successful comparison between a filter and the packet being examined, the filtering process stops and the forwarding action in that filter is applied to the packet.

If no comparison succeeds, the packet does not match the filter. However, this does not mean that the packet is forwarded. When no filter is in use, the DSL Terminator unit forwards all packets, but applying a filter to an interface reverses this default. For security purposes, the unit does not automatically forward nonmatching packets. It requires a filter that explicitly allows such packets to pass. (For a sample input filter that forwards packets that did not match a previous filter, see "Examples of an IP filter to prevent local address spoofing" on page 11-14.)

Note: For a call filter to prevent an interface from remaining active unnecessarily, you must define filters for both input and output packets. Otherwise, if only input filters are defined, output packets will keep a connection active, or vice versa.

Generic filters

In a generic filter, all of the settings in a filter specification work together to specify a location in a packet and a number to be compared to that location. The type of comparison that constitutes a match (equal or not-equal) must also be specified. When a comparison fails, the packet undergoes the next comparison. When a comparison succeeds, the filtering process stops and the forwarding action in that filter is applied to the packet.

If a generic filter is applied as a call filter and a comparison succeeds, the forwarding action is either to reset the idle timer or not, depending on how the filter is defined. If a generic filter is applied as a data filter, the forwarding action is either to forward the packet or drop it.

IP filters

In an IP filter, each filter specification includes a set of comparisons that are made in a defined order. When a comparison fails, the packet undergoes the next comparison. When a comparison succeeds, the filtering process stops and the forwarding action in that filter is applied to the packet. The IP filter tests proceed in the following order:

1 Apply the Src Mask value to the Src Adrs value and compare the result to the source address of the packet. If they are not equal, the comparison fails.

2 Apply the Dst Mask value to the Dst Adrs value and compare the result to the destination address in the packet. If they are not equal, the comparison fails.

3 If the Protocol parameter is zero (which matches any protocol), the comparison succeeds. If it is nonzero and not equal to the protocol field in the packet, the comparison fails.

4 If the Src Port Cmp parameter is not set to None, compare the Src Port # number to the source port number of the packet. If they do not match as specified by the Src Port Cmp parameter, the comparison fails.

5 If the Dst Port Cmp parameter is not set to None, compare the Dest Port # number to the destination port number of the packet. If they do not match as specified by the Dst Port Cmp parameter, the comparison fails.

6 If TCP Estab is set to Yes and the protocol number is 6, the comparison succeeds.

If an IP filter is applied as a call filter and a comparison succeeds, the forwarding action is either to reset the idle timer or not, depending on how the filter is defined. If an IP filter is applied as a data filter, the forwarding action is either to forward the packet or drop it.

Type of Service filters

In an IP TOS filter, each filter specification includes a set of comparisons that are made in a defined order. When a comparison fails, the packet undergoes the next comparison. When a comparison succeeds, the filtering process stops and the action specified in that filter is applied to the packet. The TOS filter tests proceed in the following order:

1. Apply the Src Mask value to the Src Adrs value and compare the result to the source address of the packet. If they are not equal, the comparison fails.
2. Apply the Dst Mask value to the Dst Adrs value and compare the result to the destination address in the packet. If they are not equal, the comparison fails.
3. If the Protocol parameter is zero (which matches any protocol), the comparison succeeds. If it is nonzero and not equal to the protocol field in the packet, the comparison fails.
4. If the Src Port Cmp parameter is not set to None, compare the Src Port # number to the source port number of the packet. If they do not match as specified by the Src Port Cmp parameter, the comparison fails.
5. If the Dst Port Cmp parameter is not set to None, compare the Dest Port # number to the destination port number of the packet. If they do not match as specified by the Dst Port Cmp parameter, the comparison fails.

If a comparison succeeds, the system sets the precedence bits and class of service (depending on how the filter is defined) in the TOS header of the packet.

Specifying a filter's direction

A local Filter profile can define up to 12 input-filter specifications and 12 output-filter specifications. Following are the relevant parameters, shown with their default settings:

```
Ethernet
  Filters
    Filter profile
      Name
      Input Filters...
        In Filter (1-12)
          Valid=No
      Output Filters...
        Out Filter (1-12)
          Valid=No
```

Parameter	Specifies
Name	Name of a Filter profile. For details, see "Example of applying a filter to a LAN interface" on page 11-26.
Input Filters (1–12)	Each filter can contain up to 12 input-filter specifications, which are defined individually and applied in order (1–12) to the inbound packet stream. The order in which the input filters are defined is significant.

Parameter	Specifies
Output Filters (1–12)	Each filter can contain up to 12 output-filter specifications, which are defined individually and applied in order (1–12) to the outbound packet stream. The order in which the output filters are defined is significant.
Valid	Enable/disable the filter specification. With a setting of No (the default), the specification is skipped when filtering the data stream. Set this parameter Yes for each defined filter you intend to use.

In a RADIUS profile, each filter is specified separately by using the Ascend-Data Filter and Ascend-Call Filter attributes. As is always the case with filters, the order in which they are applied within the user profile is significant.

In a RADIUS filter definition, you specify the direction in which to monitor the data stream as `in` or `out`. This specification provides the same function as the Input Filters and Output Filters parameters in a local profile. The following example shows an input-filter definition in RADIUS.

```
test-user Password="test-pw"
    Ascend-Data Filter="ip in forward tcp dstport > 1023"
```

Specifying a filter's forwarding action

For generic, IP, each input or output filter in a local Filter profile specifies a forwarding action for packets that match the filter. Following is the relevant parameter (shown with its default settings):

```
Ethernet
  Filters
    Filter profile
      Name
      Input Filters...
        In Filter (1-12)
          Generic...
            Forward=No
      Output Filters...
        Out Filter (1-12)
          Generic...
            Forward=No
```

Parameter	Specifies
Forward	The forwarding action for the filter. When no filters are in use, the DSL Terminator unit forwards all packets by default. When a filter is in use, the default is to discard matching packets (Forward=No).

Note: For Type of Service filters, the forwarding action has no effect. Those filters perform a different type of action on matching packets.

In a RADIUS definition, you specify the action a filter takes as `forward` or `drop`. This specification provides the same function as the Forward parameter in a local profile. The following example shows an input filter whose forwarding action is to drop matching packets.

```
test-user Password="test-pw"
    Ascend-Data Filter="ip in drop tcp dstport > 1023"
```

Defining generic filters

Generic filters can match any packet, regardless of its protocol type or header fields. The filter specifications operate together to define a location in a packet and a hexadecimal value to compare to it.

Settings in a local Filter profile

In a local Filter profile, a generic filter uses the following parameters (shown with their default values):

```
Input filters...
  In filter NN
    Generic...
      Offset=0
      Length=0
      Mask= 00:00:00:00:00:00:00:00:00:00:00:00
      Value=00:00:00:00:00:00:00:00:00:00:00:00
      Compare=No
      More=No
```

The same parameters are also available in the Output Filters subprofile. If you set the parameters in an input filter, only inbound packets are examined. If you set them in an output filter, only outbound packets are examined.

Parameter	Specifies
Offset	Byte-offset at which to start comparing packet contents to the Value setting specified in the filter. For details, see “Specifying the offset to the bytes to be examined” on page 11-8.
Length	Number of bytes to test in a packet, starting with the byte at the specified Offset parameter. For details, see “Specifying the number of bytes to test” on page 11-8.
Mask	A binary mask.The system applies the Mask to the value specified by the Value parameter before comparing it to the bytes in a packet specified by the Offset parameter. For details, see “Masking the value before comparison” on page 11-9.
Value	A hexadecimal number to be compared to the packet data identified by the Offset, Length, and Mask calculations. After you have entered the number, the system enters a colon at the byte boundaries.

Parameter	Specifies
Compare	Type of comparison to perform. If Compare is set to Yes, the comparison succeeds (the filter matches) if the contents do not equal the specified value. For a filter that requires the packet contents to equal the specified value, leave Compare set to No.
More	Enable/disable application of the next filter before determining whether the packet matches the specification. If More is set to Yes, the current specification is linked to the one immediately following it, so the filter can examine multiple noncontiguous bytes within a packet before the forwarding decision is made. The match occurs only if *both* specifications are matched. (The subsequent specification must be enabled, or the DSL Terminator unit ignores the filter specification in which More is set to Yes.

Settings in a RADIUS profile

In a RADIUS profile, you define a generic filter by assigning a value to the Ascend-Call Filter or Ascend-Data Filter attribute, using the following format:

"generic *dir action offset mask value compare* [more]"

Keyword or argument	Value
generic	Type of filter. Valid filter types for the Ascend-Data Filter and Ascend-Call Filter attributes are Generic Filter (the default) and IP Filter.
dir	Specifies direction of the packets. You can specify in (to filter packets coming in to the DSL Terminator unit or out (to filter packets going out of the DSL Terminator unit).
action	Defines the action that the DSL Terminator unit takes with a packet that matches the filter. You can specify either forward or drop.
offset	Byte-offset in a packet at which to start comparing packet contents to the *value* specified in the filter. For details, see “Specifying the offset to the bytes to be examined” on page 11-8.
mask	A binary mask. The system applies the *mask* to the specified *value* before comparing it to the bytes specified by *offset*. For details, see “Masking the value before comparison” on page 11-9.
value	A hexadecimal number to compare to the packet contents at the specified offset. The length of the number must be the same as the length of the mask (up to 12 bytes).
compare	A comparison operator that determines how the DSL Terminator unit compares packet contents to the filter value. You can specify = (Equal) or != (Not Equal). Equal is the default.

Keyword or argument	Value
more	If the `more` flag is present, the DSL Terminator unit applies the next filter specification in the profile to the current packet before deciding whether to forward or drop the packet. The direction and forwarding action of the next filter must be the same as the current filter, or the DSL Terminator unit ignores this flag.

Specifying the offset to the bytes to be examined

The offset in a generic filter is a byte-offset from the start of a packet to the start of the data in the packet to be tested. For example, with the following filter specification:

```
Input Filters
  In Filter NN
    Generic...
      Offset=2
      Length=8
      Mask=0f:ff:ff:ff:00:00:00:f0:00:00:00:00
      Value=07:fe:45:70:00:00:00:90:00:00:00:00
      Compare=no
      More=no
```

or comparable RADIUS filter definition:

```
Ascend-Data Filter="generic in drop 2 0fffffff000000f 07fe45700000009"
```

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 because of the two-byte offset.

Specifying the number of bytes to test

In a RADIUS profile, the length of the mask and value must be equal, and the system tests that number of bytes in the packet, starting at the specified offset. In a local Filter profile, the Len setting specifies the number of bytes to test in a packet, starting with the byte specified by the Offset parameter. The Mask setting is assumed have the same number of octets as the data specified by the Length parameter.

For example, with the following filter specification:

```
Input Filters
  In Filter NN
    Generic...
      Offset=2
      Length=8
      Mask=0f:ff:ff:ff:00:00:00:f0:00:00:00:00
      Value=07:fe:45:70:00:00:00:90:00:00:00:00
      Compare=no
      More=no
```

and the following packet contents:

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

the filter test the value of bytes three (97) through ten (99).

Masking the value before comparison

A generic filter can include a mask to apply to the value specified by the Value parameter before the DSL Terminator compares it to the bytes starting at the specified offset. You can use the mask to specify exactly which bits you want to compare. The mask is assumed to have the same number of octets as the data specified by the Length parameter.

The DSL Terminator unit translates both the mask and the value specified by the Value parameter into binary format and then applies a logical AND to the results. Each binary 0 (zero) in the mask hides the bit in the corresponding position in the value. A mask of all ones (FF:FF:FF:FF:FF:FF:FF:FF) masks no bits, so the full specified value must match the packet contents. For example, with the following filter specification:

```
Input Filters
  In Filter NN
    Generic...
      Offset=2
      Length=8
      Mask=0f:ff:ff:ff:00:00:00:f0:00:00:00:00
      Value=07:fe:45:70:00:00:00:90:00:00:00:00
      Compare=no
      More=no
```

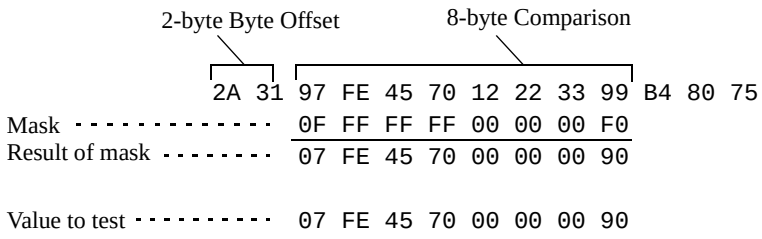
or comparable RADIUS filter definition:

```
Ascend-Data Filter="generic in drop 2 0fffffff000000f 07fe45700000009"
```

and the following packet contents:

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

The value setting matches the packet data after application of the mask.



Assuming that the Forward parameter is set to No, the packet is dropped because it matches this filter. The byte comparison works as follows:

- The DSL Terminator ignores 2A and 31 because of the two-byte offset.
- The 9 in the third byte is also ignored, because the mask has a 0 (zero) in its place. The 7 in the third byte matches the Value parameter's 7 for that byte.

- In the fourth byte, F and E match the fourth byte specified by the Value parameter.
- In the fifth byte, 4 and 5 match the fifth byte specified by the Value parameter.
- In the sixth byte, 7 and 0 match the sixth byte specified by the Value parameter.
- The seventh (12), eighth (22), and ninth (33) bytes are ignored because the mask has zeroes in those places.
- In the tenth byte, 9 matches the Value parameter's 9 for that byte. The second 9 in the of the packet's tenth byte is ignored because the mask has a 0 (zero) in its place.

Examples of a generic call filter

The following example shows how to define a generic call filter. The filter's purpose is to prevent inbound packets from resetting the session-timer.

In the Input Filter, the default values are left unchanged in the Generic Filter subprofile, so all packets are matched. Also, the forwarding action is left at its default of No. In the Output Filter, the default values again match all packets, but the forwarding action is set to Yes. So the filter does not prevent outbound packets from resetting the timer or placing a call.

```
Input filters...
  In filter NN
    Valid=Yes
    Generic...
      Forward=No
Output filters...
  Out filter NN
    Valid=Yes
    Generic...
      Forward=Yes

Following is a comparable RADIUS filter definition:
test-user Password="test-pw"
    Ascend-Call Filter="generic in drop"
    Ascend-Call Filter="generic out forward"
```

Defining IP filters

IP filters affect only IP and related packets. They make use of high-level information in packets (for example, protocol numbers, logical addresses, and TCP or UDP ports).

Settings in a local Filter profile

The IP Filter subprofile contains the following parameters (shown with their default values):

```
Input Filters
  In Filter NN
    Type=Generic
    IP...
      Src Mask=0.0.0.0
      Src Adrs=0.0.0.0
```

```
Dst Mask=0.0.0.0
Dst Adrs=0.0.0.0
Protocol=
Src Port Cmp=None
Src Port #=0
Dst Port Cmp=None
Dst Port #=0
TCP Estab=No
```

The same parameters are also available in the Output Filters subprofile. If you set the parameters in an input filter, only inbound packets are examined. If you set them in an output filter, only outbound packets are examined.

Parameter	**Specifies**
Type	Type of filter. Valid values are Generic-Filter (the default), IP-Filter, and TOS-Filter. Only the parameters in the corresponding subprofile will be applicable.
Src Mask	A mask to be applied to the Src Adrs value before comparing that value to the source address of a packet.
Src Adrs	An IP address. After applying the Src Mask value, the DSL Terminator unit compares the result to the source address in a packet. For details, see “Filtering by source or destination address” on page 11-13.
Dst Mask	A mask to be applied to the Dst Adrs value before comparing that value to the destination address of a packet.
Dst Adrs	An IP address. After applying the Dst Adrs-Mask value, the DSL Terminator unit compares the result to the source address in a packet.For details, see “Filtering by source or destination address” on page 11-13.
Protocol	A protocol number. A number of 0 (zero) matches all protocols. If you specify a nonzero number, the DSL Terminator unit compares it to the Protocol field in each packet. For a list of assigned protocol numbers, see RFC 1700, *Assigned Numbers*, by Reynolds, J. and Postel, J., October 1994.
Src Port Cmp	Type of comparison to perform when comparing source port numbers. With a setting of None (the default), no comparison is made. You can specify that the filter matches the packet if the packet’s source port number is Less (less than), Eql (equal to), Gtr (greater than), or Neq (not equal to) the Src Port # value.
Src Port #	A port number to be compared with the source port of a packet. TCP and UDP port numbers are typically assigned to services. For more details, see “Filtering by port numbers” on page 11-14.
Dst Port Cmp	Type of comparison to perform when comparing destination port numbers. With a setting of None (the default), no comparison is made. You can specify that the filter matches the packet if the packet’s destination port number is Less (less than), Eql (equal to), Gtr (greater than), or Neq (not equal to) the Dest Port # value.

Parameter	Specifies
Dest Port #	A port number to be compared with the destination port of a packet. TCP and UDP port numbers are typically assigned to services. For more details, see “Filtering by port numbers” on page 11-14.
TCP Estab	Enable/disable application of the filter only to packets in an established TCP session. Applicable only if the protocol number has been set to 6 (TCP).

Settings in a RADIUS profile

In a RADIUS profile, you define an IP filter as a value to the Ascend-Call Filter or Ascend-Data Filter attribute, using the following format:

"ip *dir action* [dstip *n.n.n.n/nn*] [srcip *n.n.n.n/nn*][*proto*] [destport *cmp value*] [srcport *cmp value*] [est]]"

Note: A filter specification cannot contain newline indicators. The syntax is shown here on two lines for printing purposes only.

Keyword or Argument	Value
ip	Type of filter. Valid filter types for the Ascend-Data Filter and Ascend-Call Filter attributes are Generic Filter (the default) and IP Filter.
dir	Specifies direction of the packets. You can specify in (to filter packets coming in to the DSL Terminator unit or out (to filter packets going out of the DSL Terminator unit).
action	Defines the action that the DSL Terminator unit takes with a packet that matches the filter. You can specify either forward or drop.
dstip *n.n.n.n/nn*	If the dstip keyword is followed by a valid IP address, the filter will match only packets with that destination address. If a subnet mask portion of the address is present, the DSL Terminator unit compares only the masked bits. If the dstip keyword is followed by the zero address (0.0.0.0), or if this keyword and its IP address specification are not present, the filter matches all IP packets. For more details, see “Filtering by source or destination address” on page 11-13.
srcip *n.n.n.n/nn*	If the srcip keyword is followed by a valid IP address, the filter will match only packets with that source address. If a subnet mask portion of the address is present, the DSL Terminator unit compares only the masked bits. If the srcip keyword is followed by the zero address (0.0.0.0), or if this keyword and its IP address specification are not present, the filter matches all IP packets. For more details, see “Filtering by source or destination address” on page 11-13.

Keyword or Argument	Value
`proto`	A protocol number. A value of zero matches all protocols. If you specify a nonzero number, the DSL Terminator unit compares it to the Protocol field in packets. For list of protocol numbers, see RFC 1700.
`dstport` *`cmp value`*	If the `dstport` default font space keyword is followed by a comparison symbol and a number, the number is compared to the destination port of a packet. The comparison symbol can be < (less-than),=(equal), > (greater-than), or ! = (not-equal). The port value can be one of the following names or numbers: ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514), or talk (517). For more details, see “Filtering by port numbers” on page 11-14.
`srcport` *`cmp value`*	If the `srcport` keyword is followed by a comparison symbol and a number, the number is compared to the source port of a packet. The comparison symbol can be < (less-than), = (equal), > (greater-than), or ! = (not-equal). The port value can be one of the following names or numbers: ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514), or talk (517). For more details, see “Filtering by port numbers” on page 11-14.
`est`	If the `est` flag is present, it restricts application of the filter to packets in an established TCP session. The protocol number must be set to 6 (TCP), or the flag is ignored.

Filtering by source or destination address

When you specify a source or destination address in an IP filter, the DSL Terminator unit applies the filter’s forwarding action to packets received from or sent to that address. If you also specify a subnet mask, the DSL Terminator unit applies the mask to the address value before comparing the resulting value to the source or destination address in a packet.

To apply the mask, the DSL Terminator unit translates both the mask and address values into binary format and then uses a logical AND to apply the mask to the address. The mask hides the bits whose positions match those of the binary zeroes in the mask. A mask of all zeros (the default) masks all bits. If the address value itself is also all zeros (the default), the filter matches any source or destination address. A mask of all ones (255.255.255.255) masks no bits, so the full source address for a single host is compared to the address value.

You can use the address mask to mask out the host portion of an address, for example, or the host and subnet portion, so the specification matches the address to or from any host on a given network.

Filtering by port numbers

IP filters can specify a port number to be compared to the source or destination port (or both) in a packet. A port number of zero matches nothing. TCP and UDP port numbers are typically assigned to services. For a list of well-known port assignments, see RFC 1700, *Assigned Numbers*.

Note: For security purposes, you should filter all services from outside your domain that are not required. UDP-based services make you network particularly vulnerable to certain types of security attacks.

The specified type of comparison determines when a match occurs. If no comparison operator is specified in the filter, no comparison is made. You can specify that the filter matches the packet if the packet's port number is Less (<), Eql (=), Gtr (>), or Neq (!=) the port number specified in the filter.

Examples of an IP filter to prevent local address spoofing

IP address spoofing typically occurs when a remote device illegally acquires a local address and uses it to try to break through a data filter. This section presents an example of a data filter that prevents IP address spoofing.

The sample filter first defines two input filters that drop packets whose source address is on the local IP network or is the loopback address (127.0.0.0). With these specifications, the DSL Terminator drops an inbound packet with one these source addresses. The third input filter accepts all remaining source addresses (by specifying a source address of 0.0.0.0) and forwards them to the local network.

In this example, the uses local IP network has an IP address of 10.100.50.128, with a subnet mask of 255.255.255.192. These values are just arbitrary examples.

Note: If you apply this filter to the Ethernet interface, the DSL Terminator unit drops IP packets it receives from the local LAN, and you will not be able to Telnet to the unit.

Configure the first input filter, and select IP filter. The first filter specifies the source mask and address for the local network. If an incoming packet has the local address, the DSL Terminator unit drops it instead of forwarding it to the Ethernet, because Forward is set to No (the default).

```
Input Filters
  In Filter 01
    Valid=Yes
    Type=IP
    IP...
      Src Mask=0.0.0.0
      Src Adrs=0.0.0.0
```

Configure the second input filter, select IP filter. The second filter specifies the loopback source address. If an incoming packet has the loopback address, the DSL Terminator unit drops it instead of forwarding it to the Ethernet, because Forward is set to No.

```
Input Filters...
  In Filter=02
    Valid=Yes
    Type=IP
```

```
    IP....
      Forward=No
      Src Mask=255.0.0.0
      Src Adrs=127.0.0.0
```

Configure the third input filter, setting Type to IP filter and setting Forward to Yes. Except for Forward=Yes, the third filter uses all default values. Because Forward is set to Yes, the DSL Terminator unit forwards all remaining packets (those with nonlocal source addresses) to the Ethernet.

```
Input filters...
  In filter=03
    Type=IP
    Valid=Yes
    IP....
      Forward=Yes
```

Configure the output filter, setting Type to IP filter and setting Forward to Yes. This filter specifies the source mask and address for the local network. (Packets originating on the local network should be forwarded across the WAN.)

```
Output filters...
  Out filter=01
    Type=IP
    Valid=Yes
    IP....
      Forward=Yes
      Src Mask=255.255.255.192
      Src Adrs=10.100.50.128
```

Following is a comparable RADIUS filter definition:

```
test-user Password="test-pw"
    Ascend-Data Filter="ip in drop srcip 10.100.50.128/26"
    Ascend-Data Filter="ip in drop srcip 127.0.0.0/8"
    Ascend-Data Filter="ip in forward"
    Ascend-Data Filter="ip out forward srcip 10.100.50.128/26"
```

Examples of an IP filter for more complex security issues

This section illustrates some of the issues you might need to consider when writing your own IP filters. However, the sample filter presented here does not address the fine points of network security. You might want to use this filter as a starting point and augment it to address your security requirements.

In this example, the local network supports a Web server, and the administrator needs to carry out the following tasks:

- Provide dial-in access to the server's IP address
- Restrict dial-in traffic to all other hosts on the local network

However, many local IP hosts need to dial out to the Internet and use IP-based applications such as Telnet or FTP, so their response packets need to be directed appropriately to the originating host. In this example, the Web server's IP address is 10.9.250.5. The filter will be applied in Connection profiles as a data filter.

Configure the first input filter, setting Type to IP Filter and setting Forward to Yes. Configure the first filter to allow packets to reach the Web server's destination address at a destination TCP port that can be used for Telnet or FTP:

```
Input filters...
  In filter=01
    Type=IP
    Valid=Yes
      IP....
      Forward=Yes
        Protocol=6
        Dst Mask=255.255.255.255
        Dst Adrs=10.9.250.5
        Dst Port Comp=Eql
        Dst Port #=80
```

Configure the second input filter, setting Type to IP and setting Forward to Yes. This allows inbound TCP packets in response to a local user's outbound Telnet request, by specifying that TCP packets whose destination port number is greater than that of the source port are forwarded. (Telnet requests go out on port 23, and responses come back on some random port above port 1023.)

```
Input filters...
  In filter=02
    Type=IP
    Valid=Yes
      IP....
      Forward=Yes
        Protocol=6
        Dst Port Comp=Gtr
        Dst Port #=1023
```

Next, configure the third input filter, setting Type to IP Filter and setting Forward to Yes. This allows inbound RIP updates, by specifying that inbound UDP packets are forwarded if the destination port number is higher than that of the source port. (For example, suppose a RIP packet goes out as a UDP packet to destination port 520. The response to this request goes to a random destination port above port 1023.)

```
Input filters...
  In filter=03
    Type=IP
    Valid=Yes
      IP....
      Forward=Yes
        Protocol=17
        Dst Port Comp=Gtr
        Dst Port #=1023
```

Configure the fourth input filter, setting Type to IP filter and setting Forward to Yes. The fourth filter uses all default values, which allows unrestricted Pings and Traceroutes. Unlike TCP and UDP, ICMP does not use ports so a port comparison is unnecessary.

```
Input filters...
  In filter=04
    Type=IP
```

```
    Valid=Yes
      IP....
      Forward=Yes
```

Following are comparable RADIUS filter definitions:

```
Ascend-Data Filter="ip in forward dstip 10.9.250.5/32 dstport=80 proto
6"
Ascend-Data Filter="ip in forward dstport > 1023 proto 6"
Ascend-Data Filter="ip in forward dstport > 1023 proto 6"
Ascend-Data Filter="ip in forward"
```

Defining Type of Service filters

To enable proxy-QoS for all packets that match a specific filter specification, you can define a TOS filter locally in a Filter profile, and then apply the filter to any number of Connection profiles or RADIUS profiles. (The Filter-ID attribute can apply a local Filter profile to RADIUS user profiles.) Administrators can also define TOS filters directly in a RADIUS user profile by setting the Ascend-Filter attribute. For TOS filters, the forwarding action in the filter has no effect.

Settings in a local Filter profile

Following are the relevant Filter parameters (shown with their default settings):

```
Input filters...
  In filter NN
    Type=TOS
    IPTOS...
      Src Mask=0.0.0.0
      Src Adrs=0.0.0.0
      Dst Mask=0.0.0.0
      Dst Adrs=0.0.0.0
      Protocol=0
      Src Port Comp=None
      Src Port #=0
      Dst Port Cmp=None
      Dst Port #=0
      Precendence=000
     Type of Service=Normal
```

Parameter	Specifies
Src Mask	A mask to be applied to the Src Adrs value before comparing that value to the source address of a packet.
Src Adrs	An IP address. After applying the Src Mask value, the DSL Terminator unit compares the result to the source address in a packet. For details, see “Filtering by source or destination address” on page 11-13.
Dst Mask	A mask to be applied to the Dst Adrs value before comparing that value to the destination address of a packet.

Parameter	Specifies
Dst Adrs	An IP address. After applying the Dst Mask value, the DSL Terminator unit compares the result to the source address in a packet.For details, see “Filtering by source or destination address” on page 11-13.
Protocol	A protocol number. A value of zero matches all protocols. If you specify a nonzero number, the DSL Terminator unit compares it to the Protocol field in each packet. For list of protocol numbers, see RFC 1700.
Src Port Cmp	Type of comparison to perform when comparing source port numbers. With a setting of None (the default), no comparison is made. You can specify that the filter matches the packet if the packet’s source port number is Less (less than), Eql (equal to), Gtr (greater than), or Neq (not equal to) the Src Port # value.
Src Port #	A port number to be compared with the source port of a packet. TCP and UDP port numbers are typically assigned to services. For more details, see “Filtering by port numbers” on page 11-14.
Dst Port Cmp	Type of comparison to perform when comparing destination port numbers. With a setting of None (the default), no comparison is made. You can specify that the filter matches the packet if the packet’s destination port number is Less (less than), Eql (equal to), Gtr (greater than), or Neq (not equal to) the Dest Port # value.
Dest Port #	A port number to be compared with the destination port of a packet. TCP and UDP port numbers are typically assigned to services. For more details, see “Filtering by port numbers” on page 11-14.
Precedence	Priority level of the data stream. The three most significant bits of the TOS byte are priority bits used to set precedence for priority queuing. When TOS is enabled and the packet matches the filter, the bits can be set to one of the following values (most significant bit first): • 000—Normal priority • 001—Priority level 1 • 010—Priority level 2 • 011—Priority level 3 • 100—Priority level 4 • 101—Priority level 5 • 110—Priority level 6 • 111—Priority level 7 (the highest priority)

Parameter	Specifies
Type of Service	Type of Service of the data stream. The value of this attribute sets the four bits following the three most significant bits of TOS byte. The next four bits of the TOS byte are used to choose a link according to the type of service. When TOS is enabled and the packet matches the filter, one of the following values can be set in the packet: Normal—Normal service Cost—Minimize monetary cost Reliability—Maximize reliability Throughput—Maximize throughput Latency—Minimize delay.

Settings in a RADIUS profile

In RADIUS, a TOS filter entry is a value of the Ascend-Filter attribute. To specify TOS filter value, use the following format:

`iptos` *`dir`* `[ dstip` *`n.n.n.n/nn`* `] [ srcip` *`n.n.n.n/nn`* `][` *`proto`* `] [ destport` *`cmp value`* `] [ srcport` *`cmp value`* `][ precedence` *`value`* `] [ type-of-service` *`value`* `]`

Note: A filter definition cannot contain newline indicators. The syntax is shown here on multiple lines for printing purposes only.

Keyword or argument	Description
iptos	Specifies an IP TOS filter.
dir	Specifies direction of the packets. You can specify in (to filter packets coming in to the DSL Terminator unit or out (to filter packets going out of the DSL Terminator unit).
`dstip` *`n.n.n.n/nn`*	If the `dstip` keyword is followed by a valid IP address, the TOS filter will set bytes only in packets with that destination address. If a subnet mask portion of the address is present, the DSL Terminator unit compares only the masked bits. If the `dstip` keyword is followed by the zero address (0.0.0.0), or if this keyword and its IP address specification are not present, the filter matches all IP packets. For more details, see “Filtering by source or destination address” on page 11-13.

Keyword or argument	Description
`srcip` *`n.n.n.n/nn`*	If the `srcip` keyword is followed by a valid IP address, the TOS filter will set bytes only in packets with that source address. If a subnet mask portion of the address is present, the DSL Terminator unit compares only the masked bits. If the `srcip` keyword is followed by the zero address (0.0.0.0), or if this keyword and its IP address specification are not present, the filter matches all IP packets. For more details, see "Filtering by source or destination address" on page 11-13.
`proto`	A protocol number. A value of zero matches all protocols. If you specify a non-zero number, the DSL Terminator unit compares it to the Protocol field in packets. For list of protocol numbers, see RFC 1700.
`dstport` *`cmp value`*	If the `dstport` keyword is followed by a comparison symbol and a port, the port is compared to the destination port of a packet. The comparison symbol can be < (less-than), = (equal), > (greater-than), or ! = (not-equal). The port value can be one of the following names or numbers: ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514), or talk (517). For more details, see "Filtering by port numbers" on page 11-14.
`srcport` *`cmp value`*	If the `srcport` keyword is followed by a comparison symbol and a port, the port is compared to the source port of a packet. The comparison symbol can be < (less-than), = (equal), > (greater-than), or ! = (not-equal). The port value can be one of the following names or numbers: ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514), or talk (517). For more details, see "Filtering by port numbers" on page 11-14.
`precedence` *`value`*	Specifies the priority level of the data stream. The three most significant bits of the TOS byte are priority bits used to set precedence for priority queuing. If a packet matches the filter, the bits are set to the specified value (most significant bit first). One of the following values can be specified: 000—Normal priority 001—Priority level 1 010—Priority level 2 011—Priority level 3 100—Priority level 4 101—Priority level 5 110—Priority level 6 111—Priority level 7 (the highest priority).

Keyword or argument	Description
`type-of-service` *`value`*	Type of Service of the data stream. If a packet matches the filter, the system sets the four bits following the three most significant bits of the TOS byte to the specified value. The four bits are used to choose a link according to the type of service. One of the following values can be specified: Normal (0)—Normal service. Disabled (1)—Disables TOS. Cost (2)—Minimize monetary cost. Reliability (4)—Maximize reliability. Throughput (8)—Maximize throughput. Latency (16)—Minimize delay.

Examples of defining a TOS filter

The following examples define a TOS filter for TCP packets (protocol 6) that are destined for a single host at 10.168.6.24. The packets must be sent on TCP port 23. For incoming packets that match this filter, the priority is set at level 2. This relatively low priority, means that an upstream router that implements priority queuing may can these packets when it becomes loaded. The parameters also set TOS to prefer a low latency connection which means that the upstream router will choose a fast connection if one is available, even if it is higher cost, lower bandwidth, or less reliable than another available link.

```
Input filters...
  In filter NN
    Valid=No
    IPTos...
      Src Mask=0.0.0.0
      Src Adrs=0.0.0.0
      Dst Mask=255.255.255.255
      Dst Adrs=10.168.6.24
      Protocol=6
      Src Port Comp=Eql
      Src Port #=23
      Dst Port Cmp=None
      Dst Port #=0
      Precendence=010
      Type of Service=Latency
```

Following is a RADIUS user profile that contains a comparable filter specification:

```
jfan-pc Password="secret"
    Service-Type=Framed-User,
    Framed-Protocol=PPP,
    Framed-IP-Address=10.168.6.120,
    Framed-IP-Netmask=255.255.255.0,
```

```
Ascend-Filter="iptos in dstip 10.168.6.24/32 dstport=23 precedence
 010 type-of-service latency"
```

Note: Filter specifications cannot contain newline indicators. The preceding example shows the specification on two lines for printing purposes only.

Applying a filter to an interface

When you apply a filter to a WAN interface, it takes effect when the connection is brought up.

Packets can pass through both a data filter and call filter on a WAN interface. When both a data filter and call filter are applied to the same interface, the data filter is applied first.

Settings in local profiles

Following are the parameters related to applying a filter (shown with their default settings):

```
Ethernet
  Answer
    Use Answer As Defaults=Yes
    Session Options...
      Call Filter=0
      Data Filter=0
      Filter Persistence=No

Ethernet
  Connections
    Connection profile
      IP Options...
        TOS Filter=
      Session Options...
        Call Filter=0
        Data Filter=0
        Filter Persistence=No


Ethernet
  Filters
    Filters profile
      Name=
```

Parameter	Specifies
Call Filter	Name of a Filter profile. For details, see “Examples of applying a call filter to a WAN interface” on page 11-25. The setting in the Answer-Defaults profile is used only for RADIUS-authenticated connections that do not include a call filter.
Data Filter	Name of a Filter profile. For details, see “Examples of applying a data filter to a WAN interface” on page 11-24. The setting in the Answer-Defaults profile is used only for RADIUS-authenticated connections that do not include a data filter.
Filter Persistence	Enable/disable filter persistence across connection state changes.

Parameter	Specifies
TOS Filter	Name of a Filter profile. For details, see “Examples of applying a TOS filter to a WAN interface” on page 11-25.
Name	Name of a Filter profile. For details, see “Example of applying a filter to a LAN interface” on page 11-26.

Settings in RADIUS profiles

The following RADIUS attribute-value pairs are used to apply a filter to a WAN connection:

Attribute	Value

Ascend-Call Filter (243)	An abinary-format filter specification using one of the following formats:
	`"generic` *`dir action offset mask value compare`* `[more]"`
	`"ip` *`dir action`* `[ dstip` *`n.n.n.n/nn`* `] [ srcip` *`n.n.n.n/nn`* `][` *`proto`* `] [ destport` *`cmp value`* `] [ srcport` *`cmp value`* `] [est]]"`
	For details, see “Defining generic filters” on page 11-6 and “Defining IP filters” on page 11-10.

Ascend-Data Filter (242)	An abinary-format filter specification using one of the following formats:
	`"generic` *`dir action offset mask value compare`* `[more]"`
	`"ip` *`dir action`* `[ dstip` *`n.n.n.n/nn`* `] [ srcip` *`n.n.n.n/nn`* `][` *`proto`* `] [ destport` *`cmp value`* `] [ srcport` *`cmp value`* `] [est]]"`
	For details, see “Defining generic filters” on page 11-6 and “Defining IP filters” on page 11-10.

Ascend-Filter (90)	A string-format filter specification using the following format: `iptos` *`dir`* `[ dstip` *`n.n.n.n/nn`* `] [ srcip` *`n.n.n.n/nn`* `][` *`proto`* `] [ destport` *`cmp value`* `] [ srcport` *`cmp value`* `][ precedence` *`value`* `] [ type-of-service` *`value`* `]` For details, see “Defining Type of Service filters” on page 11-17.
Filter-ID (11)	Name of a local Filter profile that defines a data filter. The next time the DSL Terminator unit accesses the RADIUS user profile in which this attribute appears, the referenced filter is applied to the connection.

How the system uses the Answer Default parameter

When the Ethernet >Answer > Use Answer as Default parameter is set to Yes (the default), the system creates a baseline profile for RADIUS-authenticated calls by using the settings in the

Use Answer As Defaults parameter. It retrieves the caller's configured profile from RADIUS and uses the attribute-value pairs in the profile, so if the caller's profile applies a data filter or call filter (or both), the DSL Terminator unit does not use the filters applied in the Use Answer As Defaults parameter.

Attributes that are not specified in the caller's profile take their value from the Answer profile settings. So if the caller's RADIUS profile does not apply a data filter or call filter, and the Use Answer As Default parameter is set to Yes, filters applied in the Answer profile are applied to the authenticated connection.

Examples of applying a data filter to a WAN interface

When you apply a data filter, its forwarding action (forward or drop) affects the actual data stream by preventing certain packets from reaching the Ethernet from the WAN, or vice versa. Data filters do not affect the idle timer, and a data filter applied to a Connection profile does not affect the answering process. In the following examples, the DSL Terminator unit supports the following Filter profile, IP Spoof:

Following is an example of applying a data filter:

```
Ethernet
  Connections
    Connection profile
      Session Options...
      Data Filter=IP Spoof
```

Following is a comparable RADIUS profile:

```
tlynch Password="secret"
    Service-Type=Framed-User,
    Framed-Protocol=MPP,
    Framed-IP-Address=10.10.10.64,
    Framed-IP-Netmask=255.255.255.0,
    Filter-Id="ip-spoof"
```

The following RADIUS profile references both local filters:

```
tlynch Password="secret"
    Service-Type=Framed-User,
    Framed-Protocol=MPP,
    Framed-IP-Address=10.10.10.64,
    Framed-IP-Netmask=255.255.255.0,
    Filter-Id="ip-spoof",
    Filter-Id="web-access"
```

As is always the case with filters, the order in which they are applied within the user profile is significant. If the DSL Terminator unit supports multiple Filter profiles with similar names, it attempts to match the first Filter profile to the characters specified in the user profile.

Following is an example of defining an antispoofing filter within the user's RADIUS profile:

```
tlynch Password="secret"
    Service-Type=Framed-User,
    Framed-Protocol=MPP,
    Framed-IP-Address=10.10.10.64,
```

```
    Framed-IP-Netmask=255.255.255.0,
    Ascend-Data Filter="ip in drop srcip 10.100.50.128/26"
    Ascend-Data Filter="ip in drop srcip 127.0.0.0/8"
    Ascend-Data Filter="ip in forward"
    Ascend-Data Filter="ip out forward srcip 10.100.50.128/26"
```

Examples of applying a call filter to a WAN interface

Call filters prevent unnecessary connection time and help the DSL Terminator unit distinguish active traffic from *noise*. By default, any traffic to a remote site triggers a call, and any traffic across an active connection resets the connection's idle timer.

The following parameters apply a filter to a WAN connection and set the idle timer to 20 seconds. If no packets get through the call filter in either direction for 20 seconds, the connection is torn down.

```
Ethernet
  Connections
    Connection profile
      Session Options...
        Call Filter=out-only
        Idle=20
```

Following is a comparable RADIUS profile:

```
bob Password="secret"
    Service-Type=Framed-User,
    Framed-Protocol=MPP,
    Framed-IP-Address=10.10.10.23,
    Framed-IP-Netmask=255.255.255.0,
    Ascend-Idle-Limit=20
    Ascend-Call Filter="generic in drop"
    Ascend-Call Filter="generic out forward"
```

Examples of applying a TOS filter to a WAN interface

TOS filters instruct the system to set priority bits and Type of Service (TOS) classes of service on behalf of customer applications. The DSL Terminator unit does not implement priority queuing, but it does set information that can be used by upstream routers to prioritize and select links for particular data streams. TOS filters specify which bits to set in the TOS header of IP packets.

The following parameters apply to a TOS filter in a Connection profile. When the incoming data stream contains packets that match the TOS filter specification, the proxy-QoS and TOS settings specified in the filter are set in those packets.

```
Ethernet
  Connections
    Connection profile
      IP Options...
        TOS Filter=
```

Following is a comparable RADIUS profile in which the TOS filter is specified by the Filter-ID attribute:

```
jfan-pc Password="johnfan"
    Service-Type=Framed-User,
    Framed-Protocol=PPP,
    Framed-IP-Address=10.168.6.120
    Framed-IP-Netmask=255.255.255.0
    Filter-ID="jfans-tos-filter"
```

Following is a RADIUS profile in which the TOS filter is specified within the profile:

```
jfan-pc Password="johnfan"
    Service-Type=Framed-User,
    Framed-Protocol=PPP,
    Framed-IP-Address=10.168.6.120
    Framed-IP-Netmask=255.255.255.0
Ascend-Filter="iptos in dstip 10.1.1.1/32 dstport=23 precedence
    010 type-of-service latency"
```

Note: Filter specifications cannot contain newline indicators. The preceding example shows the specification on two lines for printing purposes only.

Example of applying a filter to a LAN interface

Ethernet interfaces are connected routes, so call filters are not applicable. However, you can apply a data filter that affects which packets are allowed to reach the Ethernet or leave the Ethernet for another interface. A filter applied to an Ethernet interface takes effect immediately. If you change the Filter profile definition, the changes apply as soon as you save the Filter profile.

Note: Use caution when applying a filter to the Ethernet interface. You could inadvertently render the DSL Terminator unit inaccessible from the local LAN.

The following parameters apply to a filter in a local network interface:

```
Ethernet
  Mod Config
    Ether Options
      Filter
```

Index

Symbols

SECURE password 2-5, 2-10

Numerics

2nd Adrs 6-9

A

AAL5
  support for 4-31
ABRs. *See* Area Border Routers
Acct Type parameter 4-15
Active parameter 4-16, 5-8
address pool parameters 6-14
addresses, IP filters 11-13
adjacencies
  forming 7-3
  OSPF 7-4
alarm events
  coldStart 2-20
  linkDown 2-20
  linkUp 2-20
  RFC 1215 2-20
  warmStart 2-20
Alarm parameter 2-20
alarms, SNMP traps 2-20
All Port Diag parameter 2-9
Allow As Client DNS parameter 2-24
ALU
  defined 4-19
AMI line encoding 3-18
Answer profile 2-6, 4-1
  configuring 4-3
  parameters 4-2
ARA connections, disabling 4-3
area
  parameter 7-13, 7-14
  routing (OSPF) 7-5
Area Border Routers (ABRs) 7-5
AreaType parameter 7-13, 7-14
arguments
  Ascend-Bridge-Address 8-20
  Framed-Route 6-41
ARP
  inverse 6-10
  proxy 6-10
AS (Autonomous System) 7-2
  exterior protocols 7-2
  interior protocol 7-2
ASBR (Autonomous System Border Router) 7-2
Ascend Tunnel Management Protocol (ATMP) 10-8
  connections that bypass a Foreign Agent 10-23
  default route preference 6-5
  gateway mode parameters 10-16
  multi-mode agent, configuring 10-19
  RADIUS attributes for 10-5
  router and gateway mode 10-5
  router mode parameters 10-12
  VPN 10-1
Ascend-backup (176)
  nailed-up attribute 5-6
Ascend-BACP-Enable (134)
  BACP attribute 4-26
Ascend-Bridge (230)
  bridging attribute 8-19
Ascend-Bridge-Address (168)
  arguments 8-20
  bridging attribute 8-19
Ascend-Group (178)
  nailed-up attribute 5-6
Ascend-Home-Agent-IP-Addr 10-2
Ascend-Home-Agent-Password 10-8, 10-9
Ascend-Home-Agent-Password (184)
  ATMP connection attribute 10-5
Ascend-Home-Agent-UDP-Port 10-8, 10-9
Ascend-Home-Agent-UDP-Port (186)
  ATMP connection attribute 10-5
Ascend-Home-Network-Name 10-8, 10-9
Ascend-Home-Network-Name (185)
  ATMP connection attribute 10-6

Ascend-Idle-Limit (244)
  bandwidth management attribute 5-4
Ascend-Link-Compression (233)
  PPP attribute 4-22
Ascend-Maximum-Call-Duration (125)
  bandwidth management attribute 5-4
Ascend-Maximum-Time (194)
  bandwidth management attribute 5-5
Ascend-Multicast-Client (152)
  multicast forwarding attribute 9-8
Ascend-Multicast-Rate-Limit (153)
  multicast forwarding attribute 9-8
Ascend-PPP-Address (253)
  PPP attribute 4-22
Ascend-PPP-Async-Map (212)
  PPP attribute 4-22
Ascend-Primary-Home-Agent 10-8, 10-9
  ATMP connection attribute 10-6
Ascend-Secondary-Home-Agent
  ATMP connection attribute 10-6
ASE (Autonomous System External) 7-2
ASE-tag parameter 7-11, 7-16
ASE-type parameter 7-11, 7-16
async control character map 4-23
ATM
  features supported 3-3
  Frame Relay, using with 5-30
  interface
    configuring 3-9
  routed configuration 3-5
  sample configurations 3-10
ATM cards
  traffic shaping 3-12
ATM encapsulation 4-8
ATM Multiprotocol Encapsulation 5-30
ATM-Frame Relay circuit 5-30
ATMP
  Home Agent
    password 10-19
  Home router 10-15
  IP routing through gateway connections 10-15
  related RFC 10-2
ATMP Mode 10-8, 10-12, 10-15, 10-16
ATMP tunnels
  configuring 10-1
ATMP. *See* Ascend Tunnel Management Protocol 10-8
attributes
  BACP 4-26
  bandwidth management 5-4
  bridging 8-19
  for ATMP 10-5
  Foreign Agent 10-8
  limiting access to services and protocols 2-25
  multicast forwarding 9-8
  nailed-up 5-6
  PPP connection in RADIUS, for 4-22
Auth parameter (for RADIUS configuration) 1-7
Auth Port parameter (RADIUS setup) 1-7
Auth Timeout parameter (RADIUS setup) 1-7
authentication
  ATMP tunnels 10-19
  CHAP 4-18, 4-21
  OSPF 7-2
  PAP 4-18, 4-21
  protocols (PAP and CHAP) 1-2
  server 2-14
  servers 1-2
authenticationFailure trap 2-20
AuthKey parameter 7-10, 7-13, 7-15
AuthType parameter 7-10, 7-13, 7-15
Autonomous System Border Router (ASBR)
  disabling calculations 7-12
Average Line Utilization. *See* ALU

B

Backup 4-13
BACP connection
  configured in RADIUS 4-26
  setting up 4-26
bandwidth
  managing 5-4
  nailed, for Frame Relay 5-4
Bandwidth Allocation Control Protocol 4-19
Base Ch Count parameter 2-12
BDRs (backup designated routers) 7-4
  OSPF 7-4
bit rate
  for virtual circuits 3-15
bit rate for individual virtual circuits 3-14
black-hole interface 6-6
Block calls 2-7
Boot Protocol (BOOTP) requests 6-11
boot server 2-16
BOOTP Relay 6-16, 6-17
BOOTP. *See* Bootstrap Protocol
Bootstrap Protocol (BOOTP) 6-16, 6-17
Bridge 4-18
bridge group configuration 8-4, 8-7

bridge groups
egress interfaces 8-17
bridged IP routing 8-11
configuring with host routes 8-14
configuring with subnets 8-12
egress interface 8-17
egress interfaces 8-17
bridging
broadcast addresses 8-2
disadvantages 8-1
enabling 8-3
establishing 8-2
most common uses 8-1
overview 8-1
promiscuous mode 8-3
restricting multicast bridging 8-18
table 8-2
table, managing 8-3
transparent or learning 8-4
bridging connections
attributes for 8-19
bridging table 4-6
broadcast
addresses (and bridging) 8-2
IP address 6-3

C

calculating
call blocking 2-7
Call Detail Reporting (CDR) 1-4
management features 1-4
Call Filter 4-12
call filters, applying 11-2, 11-25
call management
incoming/outgoing calls, enabling/disabling 4-13
Call profiles 2-9, 2-11
call retries 2-7
Call Type 4-14
calls
dynamic address to incoming 6-25
CDR. *See* Call Detail Reporting
cell payload scrambling 3-4
Challenge-Handshake Authentication Protocol (CHAP) 1-2
authentication 4-18, 4-21
channel use 4-2
channels
specifying DS0s on E1 connection 3-18
CHAP. *See* Challenge-Handshake Authentication Protocol
CIDR (Classless Inter-Domain Routing) 7-3
circuits
NNI-NNI 5-24
UNI-NNI 5-26
UNI-UNI 5-22
Client 9-2, 9-5
Client DNS configuration 2-22
Client Pri DNS parameter 2-24, 6-18
Client Sec DNS parameter 2-24, 6-18
clients
outdated software, and fragmentation 10-4
Clock Source parameter 3-16, 3-18
coldStart alarm (SNMP) 2-20
Comm parameter 2-21
commands
pptp 10-26
Show dnstab 6-21
community string
R/W Comm 2-6
Read Comm 2-6
Compare parameter 11-7
compression
data 4-19
link, in tunnels 10-3
MS-Stac 4-19
MTU, and 10-3
setting 4-10
Stac 4-19
Stacker LZS 4-19
Van Jacobsen 4-10
configuration
BACP connection in RADIUS 4-26
bridge entries, of 8-19
Lucent unit for RADIUS 1-7
MP or MP+ connection in RADIUS 4-25
multicast forwarding 9-8
nailed E1 3-18
nailed T1 3-16
nailed-up connection in RADIUS 5-6
overview of DS3-ATM 3-7
PPP connection in RADIUS 4-22
Serial Port T1-CSU 3-16, 3-19
static IP routes 6-39
Configuration profile
SNMP Options menu 2-18
Connection profile 4-4
accounting options 4-15
encapsulation options parameters 4-6
Frame Relay circuits 5-21
Frame Relay, configuring 5-15, 5-16
gateway connections 5-16
Home Agent 10-17
IP options parameters 4-11
IP, to LNS 10-31

parameters 4-6
Session options parameters 4-12
telco options 4-13
connections
BACP 4-26
configuring IP address for 6-29
IP routing 6-24
MP or MP+ 4-24
nailed-up 5-5
PPP 4-22
specifying dial out number 4-6
consoleStateChange trap 2-20
cost
OSPF 7-4
stub areas 7-6
Cost parameter 7-10, 7-13, 7-15, 7-16

D

Data Communications Equipment, see DCE.
data compression 4-19
PPP link, for 4-23
Data Filter 4-12
data filters
applying 11-2, 11-24, 11-26
datalink. see link operations, Frame Relay
DCE 3-15
DCE N392 5-9
DCE N393 5-9
DeadInterval parameter 7-10, 7-13, 7-15
default
route, ignoring 6-10
subnet mask 6-2
default password 2-13
full access 2-2
default preference
of connected routes 6-5
Default profile 2-2
default read-write string 2-6
Default Security profile 2-5, 2-16
password 2-5
deleting nailed-up profiles 5-7
Dest parameter 2-21
Dest Port # parameter 11-12, 11-18
destination field 6-4
DHCP (Dynamic Host Configuration Protocol) 6-11
DHCP options 4-3
diagnostics, E1 line 3-20
diagnostics, T1 line 3-17
DNS 6-17
Domain Name 6-17
lists 6-18
table, valid names for 6-22
DNS. *See* Domain Name System
DO commands
restricting usage 2-10
Domain Name System (DNS)
Client DNS configuration 2-22
example configuration 2-24
global DNS configuration 2-22
parameters 2-24
setting connection-specific parameters 2-24
setting up 2-22
specifying global parameters 2-23
symbolic name 2-22
Domain Name System (DNS) parameters 2-23
Download parameter 2-10, 2-12
DownMetric 6-26
DownPreference 6-26
DRs (designated routers)
OSPF 7-4
DS0s
specifying how used 3-18
DS3-ATM card
configuring 3-4
example configurations 3-10
overview 3-3
overview of configuration 3-7
supported features 3-3
traffic shaping 3-12
DS3-ATM profile, described 3-8
Dst Adrs parameter 11-11, 11-18
Dst Mask parameter 11-11, 11-17
Dst Port Cmp parameter 11-11, 11-18
DSX cross-connect
configuring UDS3 card to connect to 3-7
DTE N392 5-9
DTE N393 5-9
dual IP 6-9
dual IP, configuring 6-34
dynamic address
incoming calls 6-25
dynamic IP addressing 6-11
address assignment 6-11
dynamic IP routes 6-4
dynamic route updates
configuring 6-43
dynamic routes 6-25

E

E1 connection
framing and encoding 3-18
G.703 3-18
nailed E1 3-18
specifying DS0s on 3-18
E1 line
configuration overview 3-18
diagnostics for 3-20
Edit All Calls parameter 2-9
Edit All Ports parameter 2-8
Edit Cur Call parameter 2-9
Edit Line parameter 2-8
Edit Own Call parameter 2-9
Edit Own Port parameter 2-8
Edit Security parameter 2-8
Edit System parameter 2-8
EGP (Exterior Gateway Protocol) 7-2
egress interface 8-17
egress interfaces, designating 8-17
Encaps options 5-17
Encaps parameter 4-3, 4-6
encapsulation
ATM 4-8, 5-30
ATM-FR_CIR 5-30
Frame Relay 4-8
MP 4-7
MP+ 4-7
PPP 4-7
encapsulation options parameters 4-6
encapsulation protocols
Frame-Relay-Circuit 5-22
GRE 10-2
Encoding 3-17, 3-19
Ethernet interface
configuring OSPF 7-12
creating IP interface 6-5
primary IP address 6-9
second IP address 6-9
examples
Frame Relay circuits 5-22, 5-24, 5-26
Frame Relay DLCI interface 5-18
Frame Relay link interface 5-12
L2TP tunneling 10-32
exterior protocols 7-2

F

field service operations, restricting 2-12
Field Service parameter 2-10
field service, restricting 2-10
Filter profile
direction, specifying 11-4
forwarding action 11-5
generic 11-6
IP 11-10
TOS (Type of Service) 11-17
filters
call filter, applying 11-2, 11-25
comparison success, defined 11-3
data filter, applying 11-2
defined 11-3
forwarding action 11-5
generic 11-1
generic, defined 11-6
Input Filters (1-12) parameters 11-4
IP 11-1, 11-10
Output Filters (1-12) parameters 11-5
persistence 11-22
RADIUS, configuring 11-5
security 1-2
session management, applying for 11-25
TOS (Type of Service) 11-17, 11-25
traffic direction to monitor 11-4
Type of Service 11-1
Valid parameter 11-5
firewalls
security 1-2
first profile 2-5
Flash RAM
and software, upgrading 1-4
Force fragmentation 10-12
Force56 parameter 4-2
Foreign Agent
ATMP gateway configuration 10-9
attributes 10-8
configuring 10-6
configuring (IP) 10-9
IP routing connection
Home Agent 10-7
parameters 10-6, 10-8
RADIUS, authentication 10-7
RADIUS, TCP/IP 10-7
FR Direct connections 5-16
FR Direct parameter 5-17
FR Type parameter 5-8
fragmentation
ATMP, preventing between agents 10-4
forcing clients to perform 10-4
outdated client software, and 10-4
prefragmentation in client software 10-5
tunnels, and 10-4
Frame Relay
backup interfaces 5-19
circuit between NNI interfaces 5-25

circuit between UNI interfaces 5-23
circuit between UNI/NNI interfaces 5-26
circuits 5-16
circuits, Encaps parameter 5-17
circuit-switching options 5-21
configuring profile for SDSL 8-13
connection parameters 5-17
Connection profile, configuring 5-15
connections 1-2
DCE 1-2
DLCI interface 5-15
DTE 1-2
nailed bandwidth requirement 5-4
NNI 1-2
NNI interface 5-14
parameters 5-7
RADIUS attributes 5-8, 5-10
specifying nailed group for SDSL 8-9
timers and event counts
DCE N392 5-9
DCE N393 5-9
DTE N392 5-9
DTE N393 5-9
N391 5-9
T391 5-9
T392 5-9
UNI-DCE link interface 5-13
UNI-DTE link interface 5-12
Frame Relay concentrator, described 5-2
Frame Relay encapsulation 4-8
Frame Relay Multiprotocol Encapsulation 5-30
Frame Relay switch operations 5-3
Frame Relay, using with ATM 5-30
Framed-MTU (12)
PPP attribute 4-22
Framed-Protocol (7)
attribute limiting access 2-25
MP and MP+ attribute 4-25
nailed-up attribute 5-6
PPP attribute 4-22
Framed-Route (22)
arguments 6-41
FRF 5-30
FRF.8 4-11, 5-30
Translation mode 5-30
Transparent mode 5-30
FT1 Caller 4-14
Full Access privileges 1-6
Full Access profile 2-2, 2-13
activating 2-3
changing password 2-4
Full Access Security profile 2-13
super-user 2-4

G

G.703 line encoding 3-18
G.703 line framing 3-18
gateway
field 6-4
mode (ATMP) 10-5
generic filters 11-6
bytes to test 11-8
Compare parameter 11-7
defined 11-3
interfaces, applying to 11-22
Length parameter 11-6
Mask parameter 11-6
masking value before comparison 11-9
More parameter 11-7
Offset parameter 11-6
offset to packet contents 11-8
RADIUS profile 11-7
Value parameter 11-6
Generic Routing Encapsulation (GRE) 10-1
Get command 2-6, 2-18
Get Next command 2-6, 2-18
GMT. *See* Greenwich Mean Time
GRE MTU 10-12, 10-17
GRE.*See* Generic Routing Encapsulation
Greenwich Mean Time (GMT) 6-18
GRF switch, tunneling to 10-4
group
nailed for SDSL 8-9
Group parameter 4-14
group, specifying nailed 3-17, 3-19
Grp Leave Delay 9-3

H

hardware-level address
and bridging 8-2
Heartbeat 9-4
Heartbeat Addr 9-4
Heartbeat Alarm Threshold 9-5
heartbeat monitoring parameters 9-4
Heartbeat Slot 9-4
Heartbeat Slot Count 9-4
Heartbeat Slot Time 9-4
HeartBeat UDP Port 9-4
HelloInterval parameter 7-10, 7-13, 7-15
Home Agent
Connection profile 10-17
gateway mode (IP) 10-17
gateway mode, configuring 10-14

in gateway mode 10-22
in router mode 10-22
router mode (IP) 10-13
router mode, configuring 10-11
host
addresses per class C subnet 6-3
requirements for 6-27
Host #1 6-18
Host #2 6-18
Host #3 6-18
host port diagnostics
restricting 2-9
host routes, summarizing in IP address pool 6-12

I

ICMP 6-5
Redirects 6-4
ICMP redirects 2-7
ICMP Redirects parameter 6-44
Idle limit 10-12, 10-16
ie0 interface 6-6
IF Adrs 6-7
IGMP
multicast trace packets 9-1
version-1 or version-2 9-1
Ignore Def Rt parameter 6-44
inactive interface 6-6
incoming calls
assigning dynamic address to 6-25
Input Filters (1-12) parameters 11-4
interface-based routing 6-7
interfaces
backups for nailed connections 5-19
DLCI 5-15
Frame Relay circuits 5-21
Internet Group Membership Protocol (IGMP). see IGMP, multicast forwarding
Inverse ARP. *See* Inverse Address Resolution Protocol
IP
and RIP-v2 6-27
Default route 6-38
hosts 2-21
interfaces, Ethernet and internal 6-5
ping 6-20
IP (Internet Protocol)
assigning two interface addresses 6-34
IP address
broadcast address 6-3
of remote interface to WAN 4-11
primary 6-9
specified for remote end station/router 6-35
zero subnets 6-3
IP address pool, setting 4-12
IP addresses
filtering 11-13
local spoofing, preventing 11-14
specifying 4-23
IP addressing, dynamic 6-11
address assignment 6-11
IP Adrs 6-9, 6-26, 6-34, 6-35
IP connections
settings 4-11
IP Direct 6-26
IP filters
address spoofing, preventing 11-14
defined 11-3, 11-10
Dest Port # parameter 11-12
destination address filtering 11-13
Dst Adrs parameter 11-11
Dst Mask parameter 11-11
Dst Port Cmp parameter 11-11
interfaces, applying 11-22
port number filtering 11-14
Protocol parameter 11-11
RADIUS profile 11-12
security uses 11-15
source address filtering 11-13
Src Adrs parameter 11-11
Src Mask parameter 11-11
Src Port # parameter 11-11
Src Port Cmp parameter 11-11
TCP Estab parameter 11-12
Type parameter 11-11
IP interface
specifying local address 6-26
IP network
configuring 6-19
parameters 6-9
IP on a subnet 6-19
IP options 4-3
IP options parameters 4-11
IP Route profile 6-38
IP routes
black-hole, loopback, reject 6-6
default preferences 6-4
Ethernet interface 6-5
ie0 interface 6-6
inactive interface 6-6
metrics 6-4
route preferences 6-4

WAN interfaces 6-6
IP routes and preferences
configuring 6-33
IP routing 1-2
BOOTP Relay 6-16, 6-17
bridged 8-11
configuring 6-25
configuring static routes 6-39
connection parameters 6-25
dual 6-9
dual IP example 6-9
dynamic route updates, configuring 6-43
ignoring default route 6-10
inverse ARP 6-10
local IP network setup 6-7
metrics 6-26
name servers 6-17
preferences 6-26
primary address 6-9
proxy ARP 6-10
second address 6-9
static 6-37
UDP checksums 6-19
WAN interfaces 6-24
IP routing table 6-4
at system startup 6-4
static and dynamic routes 6-4
IP-Route
ATMP mobile clients 10-15
iproute show command 6-5

L

L2TP
Network Server (LNS), connection to 10-31
L2TP (Layer 2 Tunneling Protocol) tunnels
LAC and LNS mode 10-28
L2TP Auth Enabled 10-30
L2TP LAC parameters 10-30
L2TP Mode 10-30
L2TP RX Window 10-30
L2TP. *See* Layer 2 Tunneling Protocol
LAC (L2TP Access Concentrator)
mode 10-28
LAN Adrs 6-7, 6-26, 6-38
LAN OSPF interfaces
designated router priority 7-10
Layer 2 Tunneling Protocol (L2TP) tunnels 10-1
client authentication 10-29
configuring 10-27
configuring for dial-in clients 10-27
flow control 10-29
for dial-in clients, configuring 10-27
LNS, configuring 10-32
learning bridge 8-4
Leased E1 3-18
Leased T1 3-16
Length parameter 11-6
Line N tunnel type 10-24, 10-30
lines
performing diagnostics for E1 3-20
performing diagnostics for T1 3-17
Link Comp parameter 4-19
link compression 4-10, 4-19
link management 5-9
link operations, Frame Relay 5-7
Link quality monitoring (LQM) 4-18
linkDown alarm (SNMP) 2-20
Link-State Advertisements (LSAs) 7-6
link-state routing algorithm 7-7
linkUp alarm (SNMP) 2-20
List Attempt 6-18
List Attempt parameter 2-23, 2-24
List Size 6-18
LNS (L2TP Network Server)
mode 10-28
local DNS table 6-22
configuring 6-22
local IP interface address
specifying 6-26
local IP network setup
configuring 6-7
Login Timeout parameter 2-15
loopback interface 6-6
LQM
setting 4-28
LQM (Link Quality Monitoring) 4-10
LQM Max 4-18
LQM Min 4-18
LQM. *See* Link quality monitoring
LSA-type 6-35, 7-11

M

MAC. *See* Media Access Control
Management 1-3
management features 1-3
Flash RAM
and software, upgrading 1-4
remote management
far-end units, configuring 1-3

terminal server command line 1-3
WAN or Ethernet activity, tracking 1-3
Management Information Base (MIB) 2-6, 2-17, 2-21
Mask parameter 11-6
MAX
operations, restricting 2-13
Max Burst Size 3-15
Max Call Duration 4-13
Maximum Receive Unit (MRU) 10-4
Maximum Receive Units (MRU) 4-18, 5-9
maximum transmission rate 3-15
Maximum Transmission Unit (MTU) 10-3
Mbone
restricting multicast bridging 8-18
Mbone Profile 9-5
Media Access Control (MAC) 8-2
physical address 8-4
Membership Timeout 9-2
Metric 4-3
metrics 6-4, 6-26
MIB. *See* Management Information Base
MIB. *See* Management Information Base
mobile node router
supporting (IP only) 10-19, 10-22
mobile node routers (IP only)
VPN
mobile node routers (IP only) 10-22
modifying nailed-up profiles 5-7
More parameter 11-7
MP encapsulation 4-7
MP or MP+ connection
configured in RADIUS 4-25
setting up 4-24
MP+ encapsulation 4-7
MRU. *See* Maximum Receive Units
MS-Stac compression 4-19
multicast
parameters 9-4
multicast backbone (MBONE) 9-1
clients, responding to 9-7
interfaces 9-3
multicasting
prioritized packet discarding 9-4
multicasting, configuring MBONE interface 9-7
multicasting, MBONE router 9-5
multicast bridging, restricting 8-18
multicast forwarding setting up 9-8
multicast router
on the WAN 9-6
multiple POPs
configuring 10-25

N

N391 5-9
Nailed connection 5-8
Nailed E1 3-18
nailed group
for SDSL connection 8-9
specifying T1 3-17, 3-19
Nailed T1 3-16
nailed-up connection
configured in RADIUS 5-6
setting up 5-5
Name 4-16
Name parameter 2-8, 2-19, 8-3
name servers
DNS 6-17
WINS 6-17
Name-Password profile
configuring 4-16
Name-Password profile parameters 4-15
NAT (Network Address Translation) 6-11
NetWare, and link compression 4-20
network
diagramming 1-1
Network-to-Network (NNI), defined 5-2
Novell's NetWare 4-20
NSSAs (Not So Stubby Areas) 7-6
OSPF 7-6
RFC 1587 7-6
Type-5 LSAs 7-6
Type-7 LSAs 7-6

O

OC3-ATM card
interface, configuring 3-9
traffic shaping 3-12
Offset parameter 11-6
Open Shortest Path First (OSPF) 6-4
configuring, WAN 7-14
disabling ASBR calculations 7-12
Ethernet interface, configuring 7-12
hierarchical area routing 7-5
link-state routing algorithm 7-7
routing parameters 7-9
routing, configuring 7-8
Operations parameter 2-8
OSPF (Open Shortest Path First)

adjacencies 7-4
AS (Autonomous System) 7-2
Autonomous System (AS) 7-2
costs 7-4
designated routers 7-4
forming adjacencies 7-3
link-state routing algorithm 7-6
LSA Type-5 7-6
NSSAs 7-6
overview 7-1
route convergence 7-1
security 7-2
SPF algorithm 7-3
stub areas 7-6
topological database 7-3
Output Filters (1-12) parameters 11-5
Own Port Diag parameter 2-9

P

PAC. *See* PPTP Access Controller
packet
bridging 1-2
packets
specifying maximum number of bytes in 4-23
PAP. *See* Password Authentication Protocol
Passwd parameter 2-8
Password 4-16, 10-8, 10-12, 10-16
for establishing bridging 8-2
Telnet 6-17
password
SECURE 2-5
changing Full Access 2-4
default full access 2-2
Default Security profile 2-5
Telnet 2-6
Password (2)
attribute limiting access 2-26
MP and MP+ attribute 4-25
nailed-up attribute 5-6
PPP attribute 4-22
Password Authentication Protocol (PAP) 1-2
authentication 4-18, 4-21
password parameters
Recv PW 4-9
Send PW 4-9
password, default 2-13
passwords
SNMP 2-18
Telnet 2-25
permanent virtual circuit(PVC), defined 5-1
phone numbers
specifying number used to dial out 4-6
physical address
and bridge table 8-2
Ping command 6-20
PNS. *See* PPTP Network Server
Point-to-Point protocol (PPP) 4-1
connections, authenticating 1-2
connections, configuring 4-16, 4-20
options 4-3
parameters 4-18
Point-to-Point-Tunneling Protocol (PPTP) 10-1
command 10-26
default route preference 6-5
tunnels for dial-in clients, configuring 10-23
tunnels, across multiple POPs 10-25
tunnels, multiple POPs, configuring 10-25
tunnels, PAC, configuring 10-24
Pool 6-26
Pool # N count 6-11
Pool # N start 6-11
Pool Count 6-15
Pool Only 6-12
Pool Start 6-15
Pool Summary 6-12
Port Diag menu 2-12
port diagnostics, restricting 2-9
PPP
encapsulating in ATM 4-30
link compression 4-10
PPP connection setting up 4-21
PPP encapsulation 4-7
PPP options 4-3
PPP over ATM 4-30
configuring 4-31
PPP over Ethernet
Ethernet interface 4-28
WAN interface 4-28
PPP. *See* Point-to-Point protocol
PPPoE. *See* PPP over Ethernet
PPTP Access Controller (PAC) 10-23
configuring 10-24
PPTP Enabled 10-24
PPTP Network Server (PNS) 10-23
PPTP PAC parameters 10-24
PPTP. *See* Point-to-Point-Tunneling Protocol
Precedence parameter 11-18
Preempt 4-13
preferences 6-26
Pri DNS parameter 2-23

primary DNS server address, setting 4-12
primary RADIUS server 2-22
Priority parameter 7-13, 7-15
privileges, obtaining 1-6
privileges, read-only 2-5
profile
  Answer 2-6
  default 2-2
  Default Security 2-5
  Security 2-8
  Security, configuring 2-10
  sharing 4-6
Profile Reqd parameter 4-3
profile, activating a 1-6
profiles
  Call 2-9
  configuring Frame Relay for SDSL 8-13
  configuring SDSL 8-9
  configuring static IP routes in dial-in user 6-42
  configuring static IP routes in pseudo-user 6-40
  Connection
    Frame Relay circuits 5-21
    IP, to LNS 10-31
  Connection profile for SDSL 8-13
  DS3-ATM 3-8
  Frame-Relay 5-7
  Full Access 2-2
  incoming sessions 2-6
  modifying or deleting nailed-up 5-7
  RADIUS
    Frame Relay circuits 5-22
    LNS, to 10-31
  RADIUS frdlink 5-10
  RADIUS permconn 5-18
  requiring use of 4-3
  Security 2-2
promiscuous mode 8-3
Prompt Format parameter 2-15
Protocol parameter 11-11, 11-18
protocol-independent bridging 8-19
protocols
  ATMP 10-1
  GRE 10-1
  IGMP 9-1
proxy ARP, inverse ARP 6-10
Proxy Mode 6-10
PVC.*See* permanent virtual circuit

Q

Q.922 address 6-10

R

R/W Comm 2-6
R/W Comm parameter 2-18
RADIUS
  Boot server 2-16
  configuring BACP connection in 4-26
  configuring Lucent unit for 1-7
  configuring MP or MP+ connection in 4-25
  configuring multicast forwarding in 9-8
  configuring nailed-up connection in 5-6
  configuring PPP connection in 4-22
  DLCI permconn profiles 5-18
  Frame Relay backup interfaces 5-19
  Frame Relay circuit examples 5-24, 5-25, 5-28
  Frame Relay circuits 5-22
  Frame Relay DLCI interface 5-18
  Frame Relay link operations 5-8, 5-10
  Frame Relay NNI 5-15
  Frame Relay UNI-DCE 5-14
  Frame Relay UNI-DTE 5-13
  frdlink profiles 5-8, 5-10
  LNS, connection to 10-31
  pseudo-user
    frdlink 5-10
  retrieving updates 2-7
  terminal server connections 2-15
RADIUS accounting
  shared secret (password) 4-15
Rate Limit 9-3, 9-5
Read Comm 2-6
Read Comm parameter 2-18
read-only privileges 2-5
RecvAuth parameter 4-18
reject interface 6-6
remote management
  disabling access 2-25
  far-end units, configuring 1-3
  restricting 2-11
Restore Cfg command 2-10, 2-12
restricting multicast bridging 8-18
RetransmitInterval parameter 7-11, 7-14
retries
  call 2-7
RFC 1483 5-30
RFC 1490 5-30
RFC 2364 4-30
RIP 6-37
  setting 4-11
RIP (Routing Information Protocol)
  hop count limit 7-1

route convergence 7-1
RIP metric
Connection profile, setting in 4-11
RIP parameter 6-43
RIP Policy parameter 6-44
Rip Preference 6-33
RIP Summary parameter 6-44
RIP-v1 6-44
enabling on Ethernet interface 6-10
recommendations 6-27
RIP-v2 6-44
enabling on Ethernet interface 6-10
recommendations 6-27
route
connections as routes 6-39
convergence, RIP vs OSPF 7-1
default route 6-38
disclosing 4-11
flooding, preventing 7-6
preferences 6-4
ways to specify static routes 6-4
Route AppleTalk 4-18
route filters
interfaces, applying to 11-22
Route IP 4-18, 6-25, 10-12
Route Line 10-24
Route line N 10-30
Route name 6-36
route preferences
configuring 6-39
router mode (ATMP) 10-5
routers
backup designated (BDRs) 7-4
designated (DRs) 7-4
routing
a terminal-server session to a PPTP server 10-26
ATM example 3-5
configurations 4-6
Routing Information Protocol (IPX RIP)
default route preference 6-5
static IP routes and 6-37
static routes and 6-39
routing policies 6-11
Boot Protocol (BOOTP) requests 6-11
DHCP (Dynamic Host Configuration Protocol) 6-11
DNS (Domain Name System) 6-11
dynamic IP addressing 6-11
NAT (Network Address Translation) 6-11
WINS (Windows Internet Name Service) 6-11
RunOSPF 7-10, 7-13, 7-14, 7-16

S

Save Cfg command 2-10, 2-12
SDSL card
configuring Connection profile for 8-13
configuring Frame Relay profile for 8-13
nailed group for connection 8-9
SDSL profile, configuring 8-9
Sec DNS parameter 2-23
Sec Domain Name 6-17
second IP address 6-9
secondary DNS server address 4-12
secondary RADIUS server 2-22
security
configuring basic 2-3
features listed 1-2
filters 1-2
firewall 1-2
qualifying hosts by IP address 2-21
servers 1-2
SNMP 1-3, 2-6
terminal server 2-15
Security menu 2-2, 2-8
Security parameter
SNMP 2-20, 2-21
Security profile 2-2, 2-8, 2-16
activating 2-13
configuring 2-10
Full Access 1-6
parameters 2-8
password 2-16
security-card authentication
specifying the security-card server 2-14
Send Auth parameter 4-18
Send PW parameter 4-18
servers
security 1-2
Session options 4-3
Session options parameters 4-12
Set command 2-6, 2-8
Shared Prof 6-17
Show dnstab command 6-21
Simple Network Management Protocol (SNMP) 1-3
alarm trap and multicasting 9-4
disabling traps 2-21
management features 1-3
Options menu 2-18
password protection, setting up 2-18
qualifying IP source 2-21
read-write community string, changing 2-6
restricting the hosts that can issue SNMP

commands 2-21
security 1-3
security parameters 2-17
security setup 2-17
Traps menu 2-18
Traps parameters 2-18
traps, setting up 2-17, 2-19
Simple Network Time Protocol (SNTP) 6-18
RFC 1305 6-18
server addresses 6-18
slot cards
DS3-ATM 3-3
UDS3 3-6
SNMP
traps 2-20
SNMP SET REQUEST packets 2-19
SNMP specifies the RADIUS server 2-22
SNMP Traps profile 2-19
SNMP. *See* Simple Network Management Protocol
SNMP. *See* Simple Network Management Protocol
SNTP. *See* Simple Network Time Protocol
socket 6-37
Source Addr 9-4
Source Mask 9-4
specifying a local IP interface address 6-26
SPF (Shortest Path First)
algorithm 7-3
spoofing local address
preventing 11-14
Src Adrs parameter 11-11, 11-17
Src Mask parameter 11-11, 11-17
Src Port # parameter 11-11, 11-18
Src Port Cmp parameter 11-11, 11-18
Stac compression 4-19
Stac compression, and NetWare 4-20
Stacker LZS compression 4-19
static
IP routes 6-37
static IP routes 6-4
Static Preference 6-33
static route 6-38
configuring 6-38
default route, configuring 6-38
dynamic route updates, configuring 6-43
parameters 6-33
route preferences, configuring 6-39
static routes
ATMP mobile clients. to 10-15
Static Rtes 6-33
Station 4-6, 8-3
names, for establishing bridging 8-2
status windows
WAN or Ethernet activity, tracking 1-3
stub areas 7-6
cost 7-6
subnet
address format for class C 6-3
zero 6-3
super-user 2-2, 2-4
super-user profile 2-13
symbolic name 2-22
Sys Diag parameter 2-9
sysConfigRadiusCmd 2-8
sysConfigRadiusStatus 2-8
syslog message 2-16
system diagnostics, restricting 2-9
system startup
building IP routing table 6-4
system-based routing 6-7
systemUseExceeded trap 2-20

T

T1 connection
nailed T1 3-16
T1 line
clocking 3-16, 3-18
configuring 3-16
diagnostics for 3-17
encoding 3-17, 3-19
T391 5-9
T392 5-9
TACACS+
accounting requests, UDP port 4-15
shared secret (password) 4-15
TCP Estab parameter 11-12
Telnet
access password protection 2-25
password, assigning 2-6
Telnet PW 2-6, 6-17
Template Connection 4-16
terminal server
connection 2-15
RADIUS connections 2-15
security, setting up 2-15
turning operation on or off 2-15
terminal server command line 1-3
Termserv command 6-21
the 6-12
topological database (OSPF) 7-3

TOS (Type of Service) filters
action (set precedence bits) 11-17
applying to interfaces 11-25
defined 11-4, 11-17
Dest Port # parameter 11-18
Dst Adrs parameter 11-18
Dst Mask parameter 11-17
Dst Port Cmp parameter 11-18
interfaces, applying to 11-22
Precedence parameter 11-18
Protocol parameter 11-18
RADIUS profile 11-19
Src Adrs parameter 11-17
Src Mask parameter 11-17
Src Port # parameter 11-18
Src Port Cmp parameter 11-18
Type of Service parameter 11-19
Traffic Shaper profile 3-12
traffic shaping 3-12
configuring 3-12
default profile 3-12
enabling 3-15
maximum tranmission rates, setting 3-15
setting priority 3-15
specifying for a virtual connection 3-15
TransitDelay 7-11
transparent bridging 8-4
traps-PDU 2-17
tunneling
ATMP authentication 10-19
fragmentation issues 10-4
GRF switch, to 10-4
link compression, and 10-3
MTU limit, explicit 10-3
UDP port for ATMP control information 10-3
Type 10-8, 10-12, 10-15, 10-16
Type of Service parameter 11-19
Type parameter 11-11
Type-5 LSAs 7-6
Type-7 LSAs 7-6

U

UDP
ATMP, port for tunnel control 10-3
Chksum 6-19
Port 10-8, 10-12
port number for ATMP connections 10-8
UDP port 10-12
UDS3 card
configuring physical link 3-7
overview 3-6
supported features 3-6, 3-7
Upd Rem Cfg 2-7
Upload parameter 2-10, 2-12
Use Answer As Default 4-2
User-Name (1)
attribute limiting access 2-26
MP and MP+ attribute 4-25
nailed-up attribute 5-6
PPP attribute 4-22
User-Service (6)
attribute limiting access 2-26
MP and MP+ attribute 4-25
nailed-up attribute 5-6
PPP attribute 4-22
User-to-Network (UNI), defined 5-1

V

valid names for 6-22
Valid parameter 11-5
Value parameter 11-6
Van Jacobsen compression 4-10, 4-19
Virtual Circuits. *See Frame Relay*
virtual circuits
setting individual bit rates 3-14
virtual connections
traffic shaper, specifying 3-15
Virtual Private Networks (VPN) 10-1
ATMP 10-1
ATMP tunnels, configuring 10-1
ATMP, connections that bypass a Foreign Agent 10-23
L2TP tunnels, configuring for dial-in clients 10-27
PPTP tunnels for dial-in clients, configuring 10-23
RFC 1701 10-1
Virtual Routers 10-33
parameters 10-35
RADIUS attributes 10-36
VJ Comp parameter 4-20
VLSM (Variable Length Subnet Masks) and OSPF 7-3
VPN. *See* Virtual Private Networks
VRouter. *See* Virtual Routers 10-33
VT100 menu
slots and ports 3-1

W

WAN 1-2

no OSPF, configuring 7-15
Telnet session 2-25
Telnet sessions, assigning 2-6
WAN Frame Relay interfaces
DLCI 5-15
paired, circuits 5-22
WAN IP interfaces
L2TP tunnel 10-31
WAN OSPF interfaces
designated router priority 7-10
WAN. *See* Wide-Area Network
warmStart alarm (SNMP) 2-20
Wide-Area Network (WAN)
interface, IP configuration 6-24
interface, IP routing 6-6
introduction 4-1
multicast backbone (MBONE)
multicasting, WAN, configuring 9-6
OSPF, configuring 7-14
routing and bridging 1-2
WINS 6-17

Z

zero subnets 6-3