Lucent Technologies
Bell Labs Innovations

Stinger® T1000 Module

Configuration Guide

For software version 9.4-185.1
December 2002

Copyright © 2001, 2002 Lucent Technologies Inc. All rights reserved.

This material is protected by the copyright laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Lucent Technologies), except in accordance with applicable agreements, contracts, or licensing, without the express written consent of Lucent Technologies. For permission to reproduce or distribute, please email your request to techcomm@lucent.com.

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.

European Community (EC) RTTE compliance

CE Hereby, Lucent Technologies, declares that the equipment documented in this publication is in compliance with the essential requirements and other relevant provisions of the Radio and Telecommunications Technical Equipment (RTTE) Directive 1999/5/EC.

To view the official *Declaration of Conformity* certificate for this equipment, according to EN 45014, access the Lucent INS online documentation library at http://www.lucentdocs.com/ins.

Safety, compliance, and warranty Information

Before handling any Lucent Access Networks hardware product, read the *Edge Access and Broadband Access 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

Lucent, the Lucent logo, and all Lucent brand and product names are trademarks or registered trademarks of Lucent Technologies Inc. Other brand and product names are trademarks of their respective holders.

Ordering Information

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

Feedback

Lucent Technologies appreciates customer comments about this manual. Please send them to techcomm@lucent.com.

Lucent Technologies

Customer Service

Product and service information, and software upgrades, are available 24 hours a day. Technical assistance options accommodate varying levels of urgency.

Finding information and software

To obtain software upgrades, release notes, and addenda for this product, log in to Lucent OnLine Customer Support at `http://www.lucent.com/support`.

Lucent OnLine Customer Support also provides technical information, product information, and descriptions of available services. The center is open 24 hours a day, seven days a week. Log in and select a service.

Obtaining technical assistance

Lucent OnLine Customer Support at `http://www.lucent.com/support` provides access to technical support. You can obtain technical assistance through email or the Internet, or by telephone. If you need assistance, make sure that you have the following information available:

- Active service or maintenance contract number, entitlement ID, or site ID
- Product name, model, and serial number
- Software version
- Software and hardware options 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

Obtaining assistance through email or the Internet

If your services agreement allows, you can communicate directly with a technical engineer through Email Technical Support or a Live Chat. Select one of these sites when you log in to `http://www.lucent.com/support`.

Calling the technical assistance center (TAC)

If you cannot find an answer through the tools and information of Lucent OnLine Customer Support or if you have a very urgent need, contact TAC. Access Lucent OnLine Customer Support at `http://www.lucent.com/support` and click `Contact Us` for a list of telephone numbers inside and outside the United States.

Alternatively, call 1-866-LUCENT8 (1-866-582-3688) from any location in North America for a menu of Lucent services. Or call +1 510-769-6001 for an operator. If you do not have an active services agreement or contract, you will be charged for time and materials.

Contents

Figures

About This Guide

The Stinger T1000 module includes two physical components:

- The T1000 line interface module (LIM) (STGR-LIM-T1000) is an integrated IP router module for Stinger units, with session termination and aggregation functionality.
- The (optional) T1000 line element module (LEM) (STGRFS-LEM-2 or STGRLS-LEM-2) provides two 10/100BaseT Ethernet interfaces for the T1000 LIM that can be used for direct IP over Ethernet egress from a Stinger unit.

Note The Stinger T1000 module is currently available only for Stinger FS, Stinger FS+, and Stinger LS platforms. It is not currently available for the Stinger RT.

Note This manual describes the full set of features for Stinger units with an installed T1000 module, running software version TAOS 9.4-185. Some features might not be available with earlier versions or specialty loads of the software.

What is in this guide

This guide describes how to configure termination and aggregation of RFC 1483 Asynchronous Transfer Mode (ATM) PVCs, PPP over Ethernet (PPPoE) sessions, and PPP over ATM (PPPoA) sessions. It also describes how to integrate bridging customer premises equipment (CPE) devices by using transparent bridging, grouped bridged interfaces, or bridged IP routing (BIR).

The following manuals are also important sources of T1000 configuration information:

- *Stinger T1000 Routing and Tunneling Supplement*—to configure IP routing and optional virtual private network (VPN) capabilities
- *Stinger ATM Configuration Guide*—to configure ATM connections

For information about configuring frame relay, to support T1000 termination of PPP sessions over frame relay, see the *Stinger IDSL 32-Port Line Interface Module (LIM) Guide*.

Warning Before installing your Stinger unit, be sure to read the safety instructions in the *Edge Access and Broadband Access Safety and Compliance Guide*. For information specific to your unit, see the "Safety-Related Electrical, Physical, and Environmental Information" appendix in the *Getting Started Guide* for your Stinger unit.

Documentation conventions

Following are the special characters and typographical conventions that might be used in this manual:

Convention	Meaning
`Monospace text`	Represents text that appears on your computer's screen, or that could appear on your computer's screen.
`Boldface monospace text`	Represents characters that you enter exactly as shown (unless the characters are also in ***`italics`***—see *Italics*, below). If you could enter the characters but are not specifically instructed to, they do not appear in boldface.
Italics	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[ ]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in boldface.
|	Separates command choices that are mutually exclusive.
>	Separates levels of profiles, subprofiles, and parameters in a pathname in a hierarchical menu when the path to a menu item is referred to in text.
:	Separates levels of profiles, subprofiles, and parameters in a pathname displayed in the command-line interface or referred to in text.
Key+Key	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.
 **Warning:**	Warns of danger of electric shock.

Stinger documentation set

The Stinger documentation set consists of the following manuals, which can be found at http://www.lucent.com/support and http://www.lucentdocs.com/ins:

- **Read me first:**
  - *Edge Access and Broadband Access Safety and Compliance Guide*. Contains important safety instructions and country-specific information that you must read before installing a Stinger unit.
  - *TAOS Command-Line Interface Guide*. Introduces the TAOS command-line environment and shows you how to use the command-line interface effectively. This guide describes keyboard shortcuts and introduces commands, security levels, profile structure, and parameter types.
- **Installation and basic configuration:**
  - *Getting Started Guide* for your unit. Shows how to install your Stinger chassis and hardware. This guide also shows you how to use the command-line interface to configure and verify IP access and basic access security on the unit, and how to configure Stinger control module redundancy.
  - Module guides. For each Stinger line interface module (LIM), trunk module, or other type of module, an individual guide describes the module's features and provides instructions for configuring the module and verifying its status.
- **Configuration:**
  - *Stinger ATM Configuration Guide*. Describes how to use the command-line interface to configure Asynchronous Transfer Mode (ATM) operations on a Stinger unit. The guide explains how to configure permanent virtual circuits (PVCs), and shows how to use standard ATM features such as quality of service (QoS), connection admission control (CAC), and subtending.
  - *Stinger Private Network-to-Network Interface (PNNI) Supplement*. Provides quick-start instructions for configuring PNNI and soft PVCs (SPVCs), and describes the related profiles and commands in the Stinger command-line interface.
  - *Stinger SNMP Management of the ATM Stack Supplement.* Describes SNMP management of ATM ports, interfaces, and connections on a Stinger unit to provide guidelines for configuring and managing ATM circuits through any SNMP management utility.
  - *Stinger T1000 Module Routing and Tunneling Supplement.* Describes how to configure IP routing and optional virtual private network (VPN) capabilities supported by a Stinger T1000 module.
- *RADIUS: TAOS RADIUS Guide and Reference*. Describes how to set up a TAOS unit to use the Remote Authentication Dial-In User Service (RADIUS) server and contains a complete reference to RADIUS attributes.
- **Administration and troubleshooting:** *Stinger Administration Guide*. Describes how to administer the Stinger unit and manage its operations. Each chapter focuses on a particular aspect of Stinger administration and operations. The chapters describe tools for system management, network management, and Simple Network Management Protocol (SNMP) management.

- **Reference**:
  - *Stinger Reference*. An alphabetic reference to Stinger profiles, parameters, and commands.
  - *TAOS Glossary*. Defines terms used in documentation for Stinger units.

Related documents

The following requests for comments (RFCs) are relevant to the TAOS software described in this guide:

- RFC 1334, *PPP Authentication Protocols.*
- RFC 1483, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*.
- RFC 1638, *PPP Bridging Control Protocol (BCP).*
- RFC 1661, *The Point-to-Point Protocol (PPP).*
- RFC 1934, *Ascend's Multilink Protocol Plus (MP+)*
- RFC 1962, *The PPP Compression Control Protocol (CCP).*
- RFC 1974, *PPP Stac LZS Compression Protocol.*
- RFC 1989, *PPP Link Quality Monitoring.*
- RFC 1990, *The PPP Multilink Protocol (MP)*
- RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP).*
- RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*.
- RFC 2516, *A Method for Transmitting PPP Over Ethernet (PPPoE).*
- RFC 2364, *PPP over AAL5.*
- RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support.*

Welcome to the Stinger T1000 Module

1

The T1000 line interface module (LIM) (STGR-LIM-T1000) is an IP termination device and router. A Stinger unit generally contains no more than two T1000 LIMs. If a system supports more than one T1000 LIM, each operates as an independent router.

The optional T1000 line element module (LEM) (STGRLS-LEM-2 or STGRFS-LEM-2) provides two 10/100 BaseT interfaces for LAN egress.

The T1000 can terminate ATM PVCs from DSL subscribers and route the reassembled IP packets onto a LAN or WAN through one of the LEM Ethernet interfaces. The T1000 can also terminate ATM PVCs from DSL subscribers, perform the IP processing, and then select an ATM trunk as the egress interface for the traffic on the basis of IP routing. In this case, the Stinger control module reencapsulates the packets for transport onto the ATM network.

By connecting directly to IP networks, the T1000 enables aggregation of edge virtual circuits. For example, with a single ATM virtual circuit from the T1000 to a destination such as an Internet Service Provider (ISP), the module can terminate RFC 1483 PVCs from DSL subscribers and route the users' IP packets out to the ISP on a single virtual circuit, without creating new virtual circuits for each subscriber connection.

Overview of T1000 connection features

The T1000 module supports the following connection features:

- Ethernet-to-WAN bridging and bridged IP routing (BIR)
- PPPoE (RFC 2516) termination of up to 992 sessions
- PPPoA (RFC 2364) termination of up to 992 sessions
- Multiprotocol over ATM (RFC 1483) PVC termination of up to 992 sessions
- RADIUS, extended RADIUS, Password Authentication Protocol (PAP), Challenge Authentication Protocol (CHAP), profile based access
- IP routing, including RIP v1/v2

- IP multicast forwarding (IGMP v1/v2)

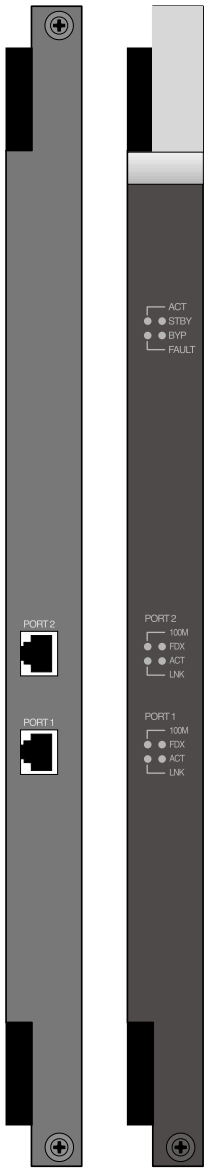
The T1000 module also supports the following optional routing and tunneling services:

- L2TP and ATMP tunneling support—requires the STGR-SP-TUNNEL software package (one per chassis)
- Virtual routing for high-density circuit termination with secure logical partitioning and multiple route tables—requires the STGR-SO-VR software option (one per chassis)

T1000 hardware specifications

Figure 1-1 shows the two physical components and lists the hardware specifications.

Figure 1-1. T1000 hardware specifications



Dimensions of each module:
Height: 15 in. (38.1 cm)
Width: 1.06 in. (2.69 cm)
Depth: 9 in. (22.8 cm)

Power Requirements:
T1000: 25 Watts
LEM: < 1 Watt

Weight:
T1000 LIM: 2.4 lb (1.1 Kg)
FS LEM: 1.0 lb (0.5 Kg)
LS LEM: 1.6 lb (0.7 Kg)

LAN Interfaces:
Dual Ethernet 10/100Base-T ports via separate LEM module

Status Indicators:
ACTIVE (Green): LIM is fully operational
STBY (Orange): Not used. Should be OFF.
BYPASS (Orange): Not used. Should be OFF.
FAULT (Orange): Fatal error detected

Status Indicators Per LAN Port:
100M (Green): Port operating in 100Mbps mode, off is 10Mbps
FDX (Green): Port operating in full duplex mode
LNK (Green): Port is linked
ACT (Green): Port has traffic activity

Operating Requirements:
Temperature: 32° – 131° F (0° – 55° C)
Relative Humidity: 10% – 90% (non-condensing)
Operating Altitude: Up to 13,123 ft (4,000 m)

Certification:
Bellcore GR-63-CORE
(NEBS Level 1-3)
Bellcore GR-1089-CORE
EN/IEC 60950

Electromagnetic Compliance:
FCC Part 15 Class A
EN55022 Class A
AS/NZS 3548 Class A
VCCI Class A
CISPR 22 Class A
EN 300386-2

T1000 module installation

The installation procedures for a T1000 module depend on which Stinger chassis you are using. The LIM is installed in a LIM slot, and the LEM must be installed in the associated line protection module (LPM) slot, following the LPM installation procedure. For example, the following commands a T1000 module, including the optional LEM, installed in slot 3:

```
admin> show
Controller { first-control-module } ( PRIMARY ):
                              Reqd  Oper  Slot Type
```

```
  { second-control-module }   UP    DOWN  ( SECONDARY )
  { shelf-1 slot-2 0 }        UP    UP    dadsl-atm-24-card
  { shelf-1 slot-3 0 }        UP    UP    terminator-card
  { shelf-1 slot-5 0 }        UP    UP    sdsl-atm-v2-card
  { shelf-1 trunk-module-1 0 } UP   UP    ds3-atm-trunk-daughter-card
  { shelf-1 trunk-module-2 0 } UP    UP    oc3-atm-trunk-daughter-card
admin> rearslotshow
Slot  Slot ID
[ 1 ] 0  Empty ( IRM, LPM )
[ 2 ] 92 24 port Enhanced LPM
[ 3 ] ea T1000 LEM card for Stinger FS/LS/RT
[ 4 ] 0  Empty ( IRM, LPM )
[ 5 ] 0  Empty ( IRM, LPM )
...
```

The T1000 cannot be used with an LPM. For details about how to install a T1000 module, see the *Getting Started Guide* for your Stinger unit. To install the LEM, follow the instructions for LPM installation.

Introduction to profiles and commands

Besides configuring the LAN or internal interfaces of the T1000 module, most of the configuration tasks are related to PPP sessions over Ethernet or ATM, ATM PVC aggregation, or IP routing and tunneling.

Configuration and status profiles

Table 1-1 lists profiles related to T1000 configuration or status, and describes where to find information about using them. In addition, all profiles have entries in the *Stinger Reference*.

Table 1-1.

Profile	Where to find details
ethernet	Chapter 2, “Configuring T1000 Interfaces” and Chapter 3, “Configuring Packet Routing and Bridging”
ip-interface	Chapter 2, “Configuring T1000 Interfaces”and the *Stinger T1000 Routing and Tunneling Supplement*
answer-defaults	Chapter 4, “Configuring PPP Session Settings”
atm-internal	Chapter 2, “Configuring T1000 Interfaces”
connection	Chapters 2 through 7 of this guide and the *Stinger T1000 Routing and Tunneling Supplement*.
l2-tunnel-global	Chapter 5, “Configuring PPP over Ethernet (PPPoE)” and the *Stinger T1000 Routing and Tunneling Supplement*
tunnel-server	

Table 1-1.

Profile	Where to find details
atmp	*Stinger T1000 Routing and Tunneling Supplement*
ip-global	
ip-route	
private-route-table	
vrouter	

Commands available at the T1000 prompt

For information about IP and VPN-related commands, see the administration appendix of the *Stinger T1000 Routing and Tunneling Supplement* or the *Stinger Reference*.

To open a session with the T1000 module, use the `open` command at the system prompt and specify the shelf and slot number of the module's physical address in the Stinger unit. For example, the following commands open a session with a module in slot 3:

```
admin> open 1 3

t1000-1/3>
```

When the session has been opened, the prompt changes to show that you are logged into the T1000 module. To end the session and return to the system prompt, use the `quit` command. For example:

```
t1000-1/3> quit
```

Following is a list of commands that are available at the T1000 prompt:

```
t1000-1/3> ?
?                               ( user )
arptable                        ( system )
auth                            ( user )
clear                           ( user )
debug                           ( diagnostic )
dnstab                          ( system )
dtunnel                         ( user )
ether-display                   ( diagnostic )
gre                             ( user )
grep                            ( user )
help                            ( user )
igmp                            ( system )
ipcache                         ( system )
ipportmap                       ( system )
l2tpsessions                    ( user )
nslookup                        ( diagnostic )
oam                             ( diagnostic )
open                            ( diagnostic )
pppif                           ( diagnostic )
```

```
quit                            ( user )
screen                          ( system )
slrt                            ( system )
version                         ( system )
vrouter                         ( system )
wanDisplay                      ( diagnostic )
wanDSess                        ( diagnostic )
wanNext                         ( diagnostic )
wanOpening                      ( diagnostic )
whoami                          ( user )
```

For details about these commands, see the *Stinger Reference*.

Configuring T1000 Interfaces 2

The T1000 module has one internal ATM interface for terminating ATM traffic the system receives on an external ATM interface. The module's internal interface has a default configuration, but you might want to change some settings or configure traffic shaper to control the bandwidth of outbound traffic directed back from the T1000 to subscribers.

The optional LEM supports two Ethernet 10/100BaseT interfaces for LAN egress. If you have installed the LEM, the system creates profiles for configuring those local interfaces.

Configuring the ATM internal interface

The system creates an `atm-internal` profile for each installed module that requires an internal interface to terminate ATM traffic—currently, the IDSL and the T1000 modules. You can set values in this profile to change the default configuration of the ATM interface, and to define traffic shapers for outbound traffic on virtual circuits that terminate on the module.

Overview of ATM internal settings

Following are the parameters, shown with default values, for configuring the internal ATM interface:

```
[ATM-INTERNAL/{ any-shelf any-slot 0 }]
name = ""
physical-address* = { any-shelf any-slot 0 }
enabled = yes

[ATM-INTERNAL/{ any-shelf any-slot 0 }:line-config]
nailed-group = 1
vp-switching-vpi = 15

[ATM-INTERNAL:traffic-shapers[1]]
enabled = no
bit-rate = 1000
peak-rate = 1000
max-burst-size = 2
```

```
aggregate = no
priority-number = 1
```

Parameter	Setting
`name`	Assigns a name to the interface, up to 15 characters. Currently, the system does not use this value for referencing the profile. It is used only for administrative purposes.
`physical-address`	Physical address of the internal ATM interface within the system. This value is set by the system when it creates the `atm-internal` profile, and it is used to retrieve the ATM configuration for the interface.
`enabled`	Enable/disable the interface for use. The interface is enabled by default.
`line-config: nailed-group`	A system-generated unique number that represents the interface in the system. You specify this number in a `connection` or RADIUS profile to terminate the connection on the T1000. **Note** With the current software version, Lucent Technologies does not recommend modifying the system-generated `nailed-group` number assigned by default to the T1000 internal interface.
`line-config: vp-switching-vpi`	*Not supported for the T1000 internal interface.*
`traffic-shapers[`*n*`]: enabled`	Enable/disable the traffic shaper for use. If a virtual circuit applies a traffic shaper that is disabled, the circuit does not come up and a warning message is displayed. (See "What happens when a traffic shaper has been disabled" on page 2-5.)
`traffic-shapers[`*n*`]: bit-rate`	Maximum sustainable effective bit rate in kilobits per second. The valid range is 1 through 135631. The default is 1000 (1Mbps). The system verifies that the `bit-rate` value of a shaper does not exceed the effective line rate.
`traffic-shapers[`*n*`]: peak-rate`	Maximum effective bit rate allowed, in kilobits per second. The valid range is 1 through 135631. The default is 1000 (1Mbps). The system verifies that the `peak-rate` value of a shaper does not exceed the effective line rate.
`traffic-shapers[`*n*`]: max-burst-size`	Maximum burst size (MBS), which is the maximum number of cells that can be transmitted at the specified peak rate before the system determines that the virtual circuit is exceeding the defined characteristics. The valid range is from 2 through 255. The default is 2.

Parameter	Setting
`traffic-shapers[n]: aggregate`	Enable/disable aggregation of virtual circuits using this traffic shaper. If the parameter set to `yes` and the traffic shaper is applied to more than one virtual circuit, the combined virtual circuits share the full bandwidth defined in the shaper.
`traffic-shapers[n]: priority-number`	Read-only numeric value, set to the number of the traffic shaper.

Example of directing traffic to the T1000 internal interface

You enable the system to direct traffic from an external ATM interface (LIM or trunk) to the T1000 internal interface by creating an ATM circuit between the two interfaces. The following command displays the `nailed-group` number assigned by the system to the internal interface of a T1000 module in slot 3:

```
admin> get atm-internal { 1 3 1 } line-config
[in ATM-INTERNAL/{ shelf-1 slot-3 1 }:line-config]
nailed-group = 101
vp-switching-vpi = 15
```

The following command displays the `nailed-group` number assigned to the fifth DSL interface in slot 5:

```
admin> which -n { 1 5 5 }
Nailed group corresponding to port { shelf-1 slot-5 5 } is 205
```

The following commands configure an ATM circuit between the sample DSL interface and the T1000 internal interface:

```
admin> new connection ckt-7
CONNECTION/ckt-7 read
admin> set active = yes
admin> set encapsulation-protocol = atm-circuit
admin> set atm-options vpi = 0
admin> set atm-options vci = 57
admin> set atm-options nailed-group = 205
admin> set atm-connect-options nailed-group = 101
admin> write
CONNECTION/ckt-7 written
```

Note You can configure an ATM circuit between any external ATM interface (LIM or trunk) and the T1000 internal interface.

User connections that terminate on the T1000 must refer to the ATM circuit profile by name in the user's `connection` profile. For example, the following profile configures an RFC 1483 PVC to terminate on the T1000:

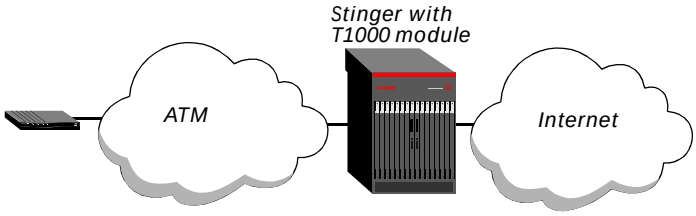
```
admin> new connection cpe-7
CONNECTION/cpe-7 read
admin> set encapsulation-protocol = atm
admin> set atm-options nailed-group = 101
```

```
admin> set atm-options atm-circuit-profile = ckt-7
admin> set ip-options remote-address = 20.0.0.1/32
admin> set active = yes
admin> write
CONNECTION/cpe-7 written
```

Example of applying traffic shapers

Figure 2-1 shows an ATM connection that will terminate on the T1000.

Figure 2-1. Example traffic shaping setup



When you define a traffic shaper in the T1000 `atm-internal` profile, the module uses the shaper definitions to limit the bandwidth of traffic directed back toward the remote unit. Because of the much higher available bandwidth on trunk interfaces, shapers are most often used on those interfaces to prevent a single application from consuming too much bandwidth.

Defining a traffic shaper

The following commands define a traffic shaper for the T1000 internal interface. The shaper limits the bit rate of traffic transmitted from that interface to less than 500Kbps (approximately 480Kbps actual transfer rate).

```
admin> read atm-internal { 1 3 1 }
ATM-INTERNAL/{ shelf-1 slot-3 1 } read
admin> set traffic-shapers 1 enabled = yes
admin> set traffic-shapers 1 bit-rate = 500
admin> list traffic-shapers 1
[in ATM-INTERNAL:traffic-shapers[1]]
enabled = yes
bit-rate = 500
peak-rate = 1000
max-burst-size = 2
aggregate = no
priority-number = 1
admin> write
ATM-INTERNAL/{ shelf-1 slot-3 1 } written
```

Note Because the traffic shaper uses the default setting for the `aggregate` parameter, the specified bit rate is applied to each individual virtual circuit to which the shaper is applied. If the traffic shaper set `aggregate` to `yes` and two virtual circuits applied the same shaper, each virtual circuit would be allowed about half the actual transfer rate, or 240Kbps.

Applying a traffic shaper to a connection

Using the sample circuit profile defined in "Example of directing traffic to the T1000 internal interface" on page 2-3, the following commands configure a subscriber connection that terminates on the T1000 and applies the traffic shaper:

```
admin> new connection cpe-1
CONNECTION/cpe-1 read
admin> set encapsulation-protocol = atm
admin> set atm-options nailed-group = 101
admin> set atm-options atm-circuit-profile = ckt-7
admin> set ip-options remote-address = 20.0.0.17/32
admin> set session-options traffic-shaper = 1
admin> set active = yes
admin> write
CONNECTION/cpe-1 written
```

What happens when a traffic shaper has been disabled

If a `connection` profile applies a traffic shaper in which the `enabled` setting has been set to `no`, the system displays log messages such as those shown below and does not establish the connection.

```
LOG info, Shelf 1, Controller-1, Time: 15:48:20--
[1/3/1/1024] Assigned to port [MBID 4]

LOG warning, Shelf 1, Slot 3, Time: 15:48:20--
[1/3/1025/0] STOP: 'cpe-1'; cause 2.; progress 2.; host 0.0.0.0 [MBID 4]
[cpe-1]
```

Configuring T1000 Ethernet interfaces

If you have installed the optional LEM, the system creates an `ethernet` profile and an `ip-interface` profile for each of the module's LAN interfaces. For example, the following command shows a T1000 module in slot 3:

```
admin> show
Controller { first-control-module } ( PRIMARY ):
                              Reqd  Oper  Slot Type
  { second-control-module }   UP    DOWN  ( SECONDARY )
  { shelf-1 slot-2 0 }        UP    UP    dadsl-atm-24-card
  { shelf-1 slot-3 0 }        UP    UP    terminator-card
  { shelf-1 slot-4 0 }        UP    UP    stngr-32-idsl-card
  { shelf-1 slot-5 0 }        UP    UP    sdsl-atm-v2-card
  { shelf-1 trunk-module-1 0 } UP    UP    ds3-atm-trunk-daughter-card
  { shelf-1 trunk-module-2 0 } UP    UP    oc3-atm-trunk-daughter-card
```

To verify that the associated LEM has been installed, use the `rearslotshow` command. For example:

```
admin> rearslotshow
Slot  Slot ID
[ 1 ] 0  Empty ( IRM, LPM )
[ 2 ] 92 24 port Enhanced LPM
```

```
[ 3 ] ea T1000 LEM card for Stinger FS/LS/RT
[ 4 ] 0  Empty ( IRM, LPM )
[ 5 ] 0  Empty ( IRM, LPM )
```

The following command shows that an ethernet profile has been created for the Ethernet interface of each control module and for those associated with the T1000 in slot 3:

```
admin> dir ethernet
    18  07/13/2001 16:50:30  { shelf-1 slot-3 1 }
    27  07/05/2001 16:23:37  { shelf-1 slot-3 2 }
    18  07/02/2001 19:30:07  { shelf-1 first-control-module 1 }
    18  07/02/2001 19:30:07  { shelf-1 second-control-module 1 }
```

The following command lists ip-interface profiles for the local interfaces on the control modules and those associated with the T1000 in slot 3:

```
admin> dir ip-interface
    18  07/02/2001 19:30:07  { { any-shelf any-slot 0 } 0 }
    32  07/20/2001 13:43:04  { { shelf-1 slot-3 1 } 0 }
    29  07/02/2001 19:34:37  { { shelf-1 slot-3 2 } 0 }
    29  07/02/2001 19:34:37  { { shelf-1 first-control-module 1 } 0 }
    29  07/02/2001 19:34:37  { { shelf-1 second-control-module 1 } 0 }
```

Ethernet link-layer configuration

The ethernet profile defines the link-layer configuration of each Ethernet interface. Following are the parameters, shown with default values, for configuring an Ethernet interface at the link layer:

```
[in ETHERNET/{ shelf-1 slot-3 1 }]
interface-address* = { shelf-1 slot-3 1 }
link-state-enabled = no
enabled = yes
ether-if-type = utp
bridging-enabled = no
filter-name = ""
duplex-mode = full-duplex
pppoe-options = { no no }
bridging-options = { 0 no }
media-speed-mbit = 100mb
auto-negotiate = no
```

Parameter	Setting
interface-address	Physical address of the interface in the Stinger unit.
link-state-enabled	Whether the link state of the interface affects the system's IP routing tables. With the default value of no, the system does not choose an alternate route if the interface is down, so packets are discarded. If the parameter is set to yes, the system deletes routes to the interface when it is down and then restores them when the interface becomes available again.
enabled	Enable/disable the interface. Ethernet interfaces are enabled by default.

Parameter	Setting
ether-if-type	Type of physical interface (read-only).
bridging-enabled	Enables/disables LAN bridging on the interface. For details, see Chapter 3, "Configuring Packet Routing and Bridging."
filter-name	Name of a data filter for this interface. Ethernet interfaces are connected routes, so call filters are not applicable.
duplex-mode	Operating mode of the interface (full-duplex or half-duplex). The default full-duplex mode provides higher throughput, but half-duplex mode enables the system to operate with older equipment that does not support full duplex. The system can determine the proper setting for this parameter when auto-negotiate is set to yes.
pppoe-options	A subprofile that enables PPPoE on the LAN interface. For details, see Chapter 5, "Configuring PPP over Ethernet (PPPoE)."
bridging-options	A subprofile that enables configuration of bridging groups. For details, see Chapter 3, "Configuring Packet Routing and Bridging."
media-speed-mbit	Operating speed of the interface (100mb or 10mb). The system can determine the proper setting for this parameter when auto-negotiate is set to yes.
auto-negotiate	Enable/disable autonegotiation on the interface. With the default no setting, the duplex-mode and media-speed-mbit settings determine operating mode and speed of the interface. When the parameter is set to yes, the interface determines the appropriate operating speed and duplex mode by using the autonegotiation protocol.

The following commands configure an Ethernet interface to use autonegotiation to determine its proper operating mode and speed, and to enable the system to use alternate routes if the interface becomes unavailable:

```
admin> read ethernet { 1 3 1 }
ETHERNET/{ shelf-1 slot-1 1 } read

admin> set auto-negotiate = yes

admin> set link-state-enabled = yes

admin> write
ETHERNET/{ shelf-1 slot-3 1 } written
```

Applying a data filter to an Ethernet interface

You can apply a data filter that affects which packets are allowed to cross the Ethernet interface in one or both directions. 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. The following commands apply a data filter to an Ethernet interface:

```
admin> read ethernet { 1 1 1 }
ETHERNET/{ shelf-1 slot-1 1 } read

admin> set filter-name = filter-dst

admin> write
ETHERNET/{ shelf-1 slot-1 1 } written
```

Use caution when applying a filter to the Ethernet interface. You could inadvertently render the system inaccessible from the local LAN. For information about defining data filters, see the *Stinger T1000 Routing and Tunneling Supplement*.

Ethernet logical-layer configuration

To enable communication on the local Ethernet segment, you must assign a local IP address to LEM interfaces. The following commands assign an IP address to an Ethernet interface:

```
admin> read ip-interface { { 1 3 1 } 0 }
IP-INTERFACE/{ { shelf-1 slot-3 1 } 0 } read

admin> set ip-address = 10.1.2.1/24

admin> write
IP-INTERFACE/{ { shelf-1 slot-3 1 } 0 } written
```

In this example, the interface is configured on the 10.1.2 subnet. To enable the system to communicate with routers on other local subnets, it must have a static route configuration to another router in its own local subnet, or the local IP interface must enable RIP. For example:

```
admin> set rip-mode = routing-recv-v2

admin> write
IP-INTERFACE/{ { shelf-1 slot-3 1 } 0 } written
```

After you assign an IP address, you can verify connectivity on that network segment by pinging another host, as shown in the following example:

```
admin> ping 10.1.2.19
PING 10.1.2.19: 56 Data bytes
64 bytes from 10.1.2.19: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 10.1.2.19: icmp_seq=3 ttl=255 time=0 ms
^C
--- 10.1.2.19: Ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

For details about IP configuration, see the *Stinger T1000 Routing and Tunneling Supplement*.

Configuring Packet Routing and Bridging

3

The T1000 module is primarily an IP termination device and router, with optional virtual private network (VPN) tunneling support. To enable the module to support connections to bridging customer premises equipment (CPE) devices and to process PPPoE packets, the module also supports packet bridging.

Packet bridging between interfaces is a resource-intensive operation. Although it is possible to use the T1000 module as a bridging device, the module has not been optimized for that purpose. To prevent a performance penalty when using the T1000 as a bridge between interfaces, Lucent Technologies recommends the following types of configuration:

- For connections to bridging CPE devices, consider using bridged IP routing. For details, see “Bridged IP routing (BIR)” on page 3-6.
- For subscriber PPPoE connections, enable the onboard PPPoE server in the T1000 module if possible and set a unique bridging group number on the ingress interface. For more details, see Chapter 5, “Configuring PPP over Ethernet (PPPoE).”
- If you must bridge subscriber PPPoE connections to an external PPPoE server, group the ingress and egress bridged interfaces to reduce bridging overhead. For more information, see “Bridging groups” on page 3-2.

IP routing and tunneling

To enable the T1000 module to route IP, you must provide some IP configuration globally and on its logical IP interfaces. You can also enable the Routing Information Protocol (RIP), or configure static routes to other routers, or both.

If the tunneling software package has been enabled in the system software, you can also configure L2TP or ATMP tunnels to remote networks.

Although this guide provides some examples of configuring routing and tunneling interfaces, the detailed information you need is located in the *Stinger T1000 Routing and Tunneling Supplement*.

Packet bridging and bridging groups

When packet bridging is enabled on multiple interfaces, the system accepts the packets it receives on a bridging-enabled interface and forwards the packets to other bridging-enabled interfaces at the data link layer, without examining the protocol information contained in the packets. To optimize its forwarding operations over time, the system uses an IEEE 802.1 transparent bridging algorithm to record the interface on which the packets reached a particular destination.

Bridging is disabled by default on local and WAN interfaces. DSL subscriber interfaces can enable bridging to allow interoperation with CPE devices that do not support routing. If both bridging and routing are enabled on an interface, the system routes packets if possible.

You can apply packet filters to control which kinds of packets are allowed to cross an interface or to reduce the amount of broadcast or multicast traffic. For details about packet filters, see the *Stinger T1000 Routing and Tunneling Supplement*.

Bridging groups

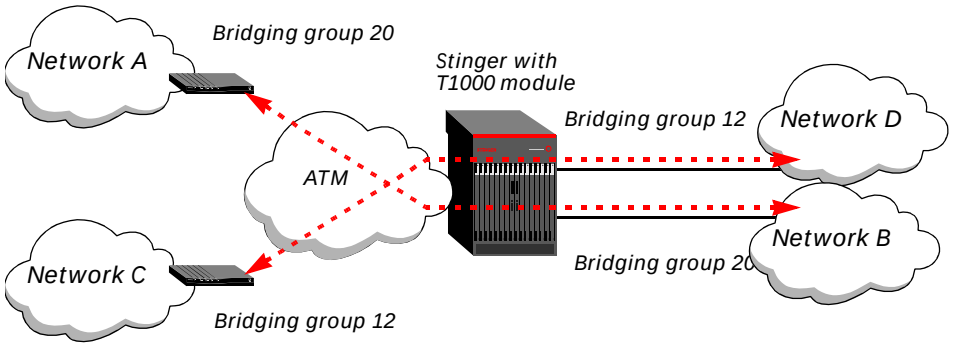
To reduce the overhead of transparent bridging operations, you can group bridged interfaces by assigning them a shared group number. When a packet is received on a bridged interface within a group, the T1000 consults the bridge logic for destination interfaces only within the same group. It does not consider interfaces in a different group as possible destinations. The effect is to isolate traffic within a set of interfaces.

For a PPPoE interface that enables the PPPoE server on the T1000 module itself, you can specify a unique `bridging-group` value on that bridged interface alone. A unique group guarantees that the module will not attempt to bridge the packets to an egress interface—an operation that is not needed when the module processes PPPoE locally.

For a PPPoE interface that does *not* enable the onboard PPPoE server (that relies instead on an external PPPoE server), you can specify a shared `bridging-group` value on the ingress and egress bridged interfaces.

Figure 3-1 shows bridging groups being used to isolate bridged traffic on specific interfaces. Interfaces to networks A and B have a `bridging-group` assignment of group 20, and interfaces to networks C and D have a `bridging-group` assignment of group 12. Traffic exchanged within one group is never forwarded to another group.

Figure 3-1. Bridging groups isolate traffic from other remote networks



Overview of parameters for enabling bridging

The following parameters, shown with default values, enable packet bridging and bridging groups:

```
[in ETHERNET/{ any-shelf any-slot 0 }]
bridging-enabled = no
```

```
[in ETHERNET/{ any-shelf any-slot 0 }:bridging-options]
bridging-group = 0
bridge = no
dial-on-broadcast = no
```

```
[in CONNECTION/"":bridging-options]
bridging-group = 0
bridge = no
dial-on-broadcast = no
```

Parameter	Setting
bridging-enabled	Enable/disable LAN packet bridging on the Ethernet interface. With LAN bridging, the system provides a direct connection between the LAN segments connected to each bridged interface.Set this parameter to yes to enable LAN bridging.
bridging-group	Number from 0 to 65535, used to group bridged interfaces. Grouping multiple bridged interfaces increases performance of the packet bridging operation and isolates traffic among those interfaces.
bridge	Enable/disable WAN packet bridging on the interface. With WAN bridging, the system can provide a connection between segments that are connected by a telecommunications link. Set this parameter to yes to enable WAN bridging.
dial-on-broadcast	*Not supported.*

The following RADIUS attribute-value pairs enable packet bridging in a RADIUS user profile:

RADIUS attribute	Value
Ascend-Bridge (230)	Enable/disable WAN packet bridging on the connection. With WAN bridging, the system can provide a connection between the local Ethernet segment and a segment across the WAN interface, or can decapsulate the Ethernet-bridged frames it receives and pass them up the protocol stack for routing. A value of Bridge-No (0) disables packet bridging. Set this attribute to Bridge-Yes (1) to enable bridging.

RADIUS attribute	Value
Ascend-BIR-Bridge-Group (7)	Number from 0 to 65535, used to group bridged interfaces. Grouping multiple bridged interfaces increases performance of the packet bridging operation and isolates traffic among those interfaces.

Enabling bridging and bridging groups on WAN interfaces

In this example, a single bridged interface to a DSL CPE is assigned a `bridging-group` number to prevent the system from bridging traffic it receives on this interface to any other interface in the system. The profile specifies an ATM circuit profile that enables it to switch the incoming traffic directly to the T1000 internal interface, as described in "Configuring the ATM internal interface" on page 2-1.

The following commands create a bridged `connection` profile:

```
admin> new connection t1000-bridge
CONNECTION/t1000-bridge read
admin> set active = yes
admin> set encapsulation-protocol = atm
admin> set ip-options ip-routing = no
admin> set bridging-options bridge = yes
admin> set bridging-options bridging-group = 1
admin> set atm-options vpi = 0
admin> set atm-options vci = 36
admin> set atm-options nailed-group = 51
admin> set atm-options atm-circuit-profile = sdsl-t1000
admin> write
CONNECTION/t1000-bridge written
```

Following is a comparable RADIUS user profile:

```
permconn-st-2 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-1483,
    User-Name = "t1000-bridge",
    Ascend-ATM-Group = 51,
    Ascend-Route-IP = Route-IP-No,
    Ascend-ATM-Vpi = 0,
    Ascend-ATM-Vci = 36,
    Ascend-Bridge = Bridge-Yes,
    Ascend-BIR-Bridge-Group = 1,
    Ascend-ATM-Circuit-Name = sdsl-t1000
```

Including Ethernet interfaces in bridging groups

Note Keep in mind that when you group a bridged LAN interface with one or more bridged WAN interfaces, you are using the T1000 module as a bridging device. This is a purpose for which the module has not been optimized, and you might therefore notice a performance penalty.

In this example, the Ethernet interfaces of a T1000 module support bridging and belong to different bridging groups. The example shows profiles for a setup such as the one shown in Figure 3-1 (page 3-2). The following commands configure the T1000 Ethernet interfaces for bridging groups:

```
admin> read ethernet { 1 3 1 }
ETHERNET/{ shelf-1 slot-3 1 } read
admin> set bridging-enabled = yes
admin> set bridging-options bridge = yes
admin> set bridging-options bridging-group = 12
admin> write
ETHERNET/{ shelf-1 slot-3 1 } read
admin> read ethernet { 1 3 2 }
ETHERNET/{ shelf-1 slot-3 2 } read
admin> set bridging-enabled = yes
admin> set bridging-options bridge = yes
admin> set bridging-options bridging-group = 20
admin> write
ETHERNET/{ shelf-1 slot-3 2 } read
```

The following commands configure WAN interfaces for PPP and bridging:

```
admin> read connection ppp-1
CONNECTION/ppp-1 read
admin> set active = yes
admin> set encapsulation-protocol = ppp
admin> set ip-options ip-routing-enabled = no
admin> set bridging-options bridge = yes
admin> set bridging-options bridging-group = 20
admin> set telco-options call-type = ft1
admin> write
CONNECTION/ppp-1 written
admin> set station = ppp-2
(New index value; will save as new profile CONNECTION/ppp-2)
admin> set bridging-options bridging-group = 12
admin> write
CONNECTION/ppp-2 written
```

Following are comparable RADIUS profiles for the WAN interfaces:

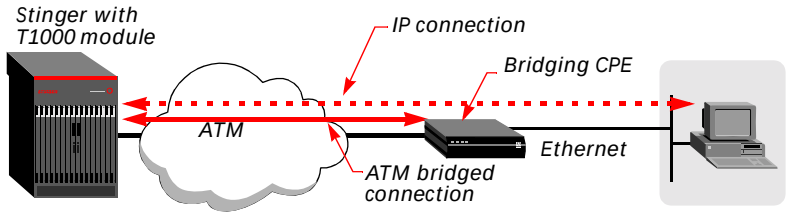
```
permconn-1 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = PPP,
    User-Name = "ppp-1",
    Framed-Routing = None,
    Ascend-Call-Type = Nailed,
    Ascend-Route-IP = Route-IP-No,
    Ascend-Bridge = Bridge-Yes,
    Ascend-BIR-Bridge-Group = 20
```

```
permconn-2 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = PPP,
    User-Name = "ppp-2",
    Framed-Routing = None,
    Ascend-Call-Type = Nailed,
    Ascend-Route-IP = Route-IP-No,
    Ascend-Bridge = Bridge-Yes,
    Ascend-BIR-Bridge-Group = 12
```

Bridged IP routing (BIR)

With Bridged IP routing (BIR), the T1000 can process IP packets encapsulated in bridged frames. BIR enables an IP host to initiate an IP connection through a CPE device that supports bridging and ATM, but not IP routing. A sample setup is shown in Figure 3-2.

Figure 3-2. IP connection through a bridging CPE



The T1000 receives the bridged packets, decapsulates them, and passes them up the protocol stack to the IP router. To the remote host, the session appears to be an ordinary IP connection.

BIR configurations require numbered interfaces, for which both the remote and local side of the connection is assigned a unique IP address. The remote address can specify a subnet or an individual remote IP host. Typically, the local address for the Stinger unit is a unique address on the remote subnet. For details about numbered interfaces, see the *Stinger T1000 Routing and Tunneling Supplement*.

Overview of BIR settings

For a complete description of the IP routing parameters in `connection` and RADIUS profiles, see the *Stinger T1000 Routing and Tunneling Supplement*. Following are the parameters, shown with default values, that are specific to BIR interfaces:

```
[in CONNECTION/"":bir-options]
enable = no
proxy-arp = no
```

```
[in CONNECTION/"":ip-options]
ip-routing-enabled = yes
remote-address = 0.0.0.0/0
local-address = 0.0.0.0/0
```

Parameter	Setting
`enable`	Enable/disable BIR on this interface.

Parameter	Setting
`proxy-arp`	Enable/disable proxy ARP, which causes the T1000 module to respond as proxy for ARP requests from local hosts for remote hosts on the far end of the link.
`ip-routing-enabled`	Enable/disable IP routing for the interface. IP routing is enabled by default.
`remote-address`	IP address of the remote device, which can include a subnet specification. If the address does not include a subnet mask, the router assumes the default subnet mask based on address class.
`local-address`	IP address assigned to the local side of a numbered-interface connection. This is a requirement for BIR interfaces. (For background information, see the *Stinger T1000 Routing and Tunneling Supplement*.)

The following RADIUS attribute-value pairs enable BIR in a RADIUS user profile:

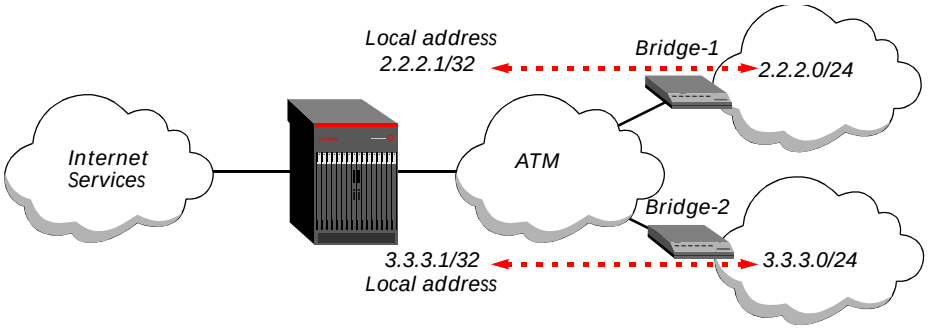
RADIUS attribute	Value
Ascend-BIR-Enable (70)	Enable/disable BIR on this interface. Set to BIR-Enable-No (0) to disable or BIR-Enable-Yes (1) to enable BIR.
Ascend-BIR-Proxy (71)	Enable/disable proxy ARP, which causes the T1000 module to respond as proxy for ARP requests from local hosts for remote hosts on the far end of the link. BIR-Proxy-No (0) disables proxy ARP. BIR-Proxy-Yes (1) enables it.
Ascend-Route-IP (228)	Enable/disable IP routing for the interface. IP routing is enabled by default.
Framed-IP-Address (8)	IP address of the calling device.
Framed-IP-Netmask (9)	Subnet mask of the caller's address. If you do not specify a subnet mask, the router assumes the default subnet mask based on address class.
Ascend-PPP-Address (253)	IP address assigned to the local side of a numbered-interface connection. This is a requirement for BIR interfaces. (For background information, see the *Stinger T1000 Routing and Tunneling Supplement*.)
Ascend-IF-Netmask (153)	Subnet mask in use for the local-side numbered interface.

Typical BIR subnet configuration

When the T1000 module receives a packet destined for a BIR subnet interface, it examines the network bits of the destination address and forwards the packet to the related CPE. For example, Figure 3-3 shows two bridging CPE devices connected to an IP class C subnet. When the T1000 receives a packet addressed to 2.2.2.200, it

examines only the first 24 bits of the address, and forwards that packet to the CPE labeled Bridge-1.

Figure 3-3. BIR subnet configurations



The following command displays the nailed-group number of the T1000 internal interface:

```
admin> get atm-internal { 1 3 1 } line-config nailed-group
[in ATM-INTERNAL/{ shelf-1 slot-3 1 }:line-config:nailed-group]
nailed-group = 101
```

BIR subnet configuration to Bridge-1

The following commands configure a BIR subnet interface to the DSL CPE bridge labeled Bridge-1 in Figure 3-3:

```
admin> new connection bridge-1
CONNECTION/bridge-1 read
admin> set active = yes
admin> set encapsulation-protocol = atm
admin> set ip-options remote-address = 2.2.2.0/24
admin> set ip-options local-address = 2.2.2.1/32
admin> set atm-options atm1483type = aal5-llc
admin> set atm-options vci = 101
admin> set bir-options enable = yes
admin> set atm-options nailed-group = 101
admin write
CONNECTION/bridge-1 written
```

Notice that the profile specifies the nailed-group number of the T1000 internal interface. Following is a comparable definition in a RADIUS profile:

```
permconn-cpe-1 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-1483,
    User-Name = "bridge-1",
    Ascend-Route-IP = Route-IP-Yes,
    Framed-IP-Address = 2.2.2.0,
    Framed-IP-Netmask = 255.255.255.0,
    Ascend-PPP-Addr = 2.2.2.1,
    Ascend-IF-Netmask = 255.255.255.255,
```

```
    Ascend-ATM-Group = 101,
    Ascend-ATM-Vci = 101,
    Ascend-BIR-Enable = BIR-Enable-Yes
```

BIR subnet configuration to Bridge-2

The following commands configure a BIR subnet interface to the DSL CPE bridge labeled Bridge-2 in Figure 3-3:

```
admin> new connection bridge-2
CONNECTION/bridge-2 read
admin> set active = yes
admin> set encapsulation-protocol = atm
admin> set ip-options remote-address = 3.3.3.0/24
admin> set ip-options local-address = 3.3.3.1/32
admin> set atm-options atm1483type = aal5-llc
admin> set atm-options vci = 102
admin> set bir-options enable = yes
admin> set atm-options nailed-group = 101
admin write
CONNECTION/bridge-2 written
```

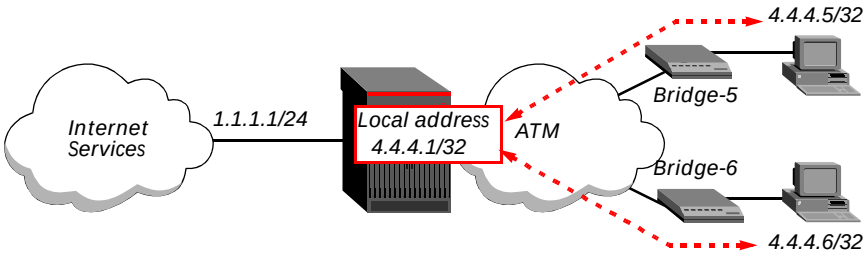
Following is a comparable definition in a RADIUS profile:

```
permconn-cpe-2 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-1483,
    User-Name = "bridge-2",
    Ascend-Route-IP = Route-IP-Yes,
    Framed-IP-Address = 3.3.3.0,
    Framed-IP-Netmask = 255.255.255.0,
    Ascend-PPP-Addr = 3.3.3.1,
    Ascend-IF-Netmask = 255.255.255.255,
    Ascend-ATM-Group = 101,
    Ascend-ATM-Vci = 102,
    Ascend-BIR-Enable = BIR-Enable-Yes
```

Typical host route (BIR/32) configurations

When the T1000 module receives a packet to a BIR/32 interface, it examines the full 32 bits of the destination address and forwards the packet to the related CPE. Figure 3-4 shows two bridging DSL CPE devices, each supporting one host. The remote hosts have addresses on the same IP network. (This is not a requirement.)

Figure 3-4. BIR/32 configurations



In Figure 3-4, the `local-address` value is the same for both BIR interfaces, which is recommended for host routes to the same IP network because it simplifies configuration of the remote hosts, all of which can point to the same local address as the gateway.

The following command displays the nailed-group number of the T1000 internal interface:

```
admin> get atm-internal { 1 3 1 } line-config nailed-group
[in ATM-INTERNAL/{ shelf-1 slot-3 1 }:line-config:nailed-group]
nailed-group = 101
```

The following commands configure a BIR/32 interface to the CPE labeled Bridge-5, and specify the T1000 nailed-group number:

```
admin> new connection bridge-5
CONNECTION/bridge-5 read

admin> set active = yes

admin> set encapsulation-protocol = atm

admin> set ip-options remote-address = 4.4.4.5/32

admin> set ip-options local-address = 4.4.4.1/32

admin> set atm-options atm1483type = aal5-llc

admin> set atm-options vci = 111

admin> set bir-options enable = yes

admin> set atm-options nailed-group = 101

admin write
CONNECTION/bridge-5 written
```

The following commands modify the previous connection profile to configure a BIR/32 interface to the CPE labeled Bridge-6:

```
admin> set station = bridge-6
(New index value; will save as new profile CONNECTION/bridge-6.)

admin> set ip-options remote-address = 4.4.4.6/32

admin> set atm-options vci = 112

admin write
CONNECTION/bridge-6 written
```

Following are comparable definitions in RADIUS profiles:

```
permconn-cpe-5 Password = "ascend"
    Service-Type = Outbound,
```

```
    Framed-Protocol = ATM-1483,
    User-Name = "bridge-5",
    Ascend-Route-IP = Route-IP-Yes,
    Framed-IP-Address = 4.4.4.5,
    Framed-IP-Netmask = 255.255.255.255,
    Ascend-PPP-Addr = 4.4.4.1,
    Ascend-IF-Netmask = 255.255.255.255,
    Ascend-ATM-Group = 101,
    Ascend-ATM-Vci = 111,
    Ascend-BIR-Enable = BIR-Enable-Yes

permconn-cpe-6 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-1483,
    User-Name = "bridge-6",
    Ascend-Route-IP = Route-IP-Yes,
    Framed-IP-Address = 4.4.4.6,
    Framed-IP-Netmask = 255.255.255.255,
    Ascend-PPP-Addr = 4.4.4.1,
    Ascend-IF-Netmask = 255.255.255.255,
    Ascend-ATM-Group = 101,
    Ascend-ATM-Vci = 112,
    Ascend-BIR-Enable = BIR-Enable-Yes
```

Configuring PPP Session Settings

4

This chapter describes general settings, such as authentication and session timers, for PPP sessions. Most of the information in this chapter applies both to local profile configuration and RADIUS external profile authentication. RADIUS supports some additional features, such as accounting, that are not described in detail here.

For information about configuring ATM WAN interfaces, see the *Stinger ATM Configuration Guide*. If you are using RADIUS to externally authenticate PPP sessions, see the *TAOS RADIUS Guide and Reference*.

Settings for on-demand PPP sessions

PPP provides a standard method of transporting multiprotocol datagrams over point-to-point links. In a Stinger unit, PPP sessions are initiated not by a dial-in call but by a packet that begins PPP negotiation.

When a Stinger unit receives an incoming PPP session request (for example, across a DSL line), it evaluates the request on the basis of the settings in the `answer-defaults` profile. If the request is acceptable, the unit looks for a `connection` or RADIUS profile to authenticate it. If it does not find a matching profile and the `answer-defaults` profile requires a profile for all session requests (the default), the unit rejects the session request.

The values in the `answer-defaults` profile are applied before the system locates the `connection` or RADIUS profile associated with the request. If the PPP client's profile contains a similar parameter with a different value, the connection-specific value overrides the `answer-defaults` value when building the session.

If you are using RADIUS authentication

For details about RADIUS authentication and configuring the Stinger unit to make use of it, see the *TAOS RADIUS Guide and Reference*. The following `answer-defaults` parameter, shown with its default value, affects baseline values used for RADIUS-authenticated session requests:

```
[in ANSWER-DEFAULTS]
use-answer-for-all-defaults = yes
```

With this default setting, the system creates a baseline default profile for RADIUS-authenticated session requests by using the settings in the `answer-defaults` profile. It retrieves the PPP client's configured profile from RADIUS and uses the attribute-value pairs in the profile. Attributes that are not specified in the profile take their values from the `answer-defaults` settings.

If `use-answer-for-all-defaults` is set to `no` and a RADIUS profile does not return certain explicit values, the system uses factory default values for RADIUS attributes instead.

Requiring PPP authentication for session requests

For PPP sessions, the authentication process is handled by access protocols such as Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). For details about those protocols, see RFC 1334, *PPP Authentication Protocols.*

During establishment of a PPP session, Link Control Protocol (LCP) packets are exchanged to negotiate the authentication protocol. After completing LCP negotiations, the T1000 module uses the agreed-upon authentication protocol to authenticate the user. It then negotiates the upper layer Network Control Protocols (NCPs) to set up the link's network-layer protocols.

The following parameters, shown with default values, affect PPP authentication of any session request:

```
[in ANSWER-DEFAULTS]
profiles-required = yes

[in ANSWER-DEFAULTS:ppp-answer]
receive-auth-mode = no-ppp-auth
```

A `profiles-required` setting of `yes` (the default) prevents unauthenticated sessions. If you set it to `no`, the system builds a temporary profile for session requests for which it cannot locate a configured profile.

To require PPP authentication for all PPP sessions, you must change the `receive-auth-mode` default. The following example specifies `any-ppp-auth` as the method of PPP authentication:

```
admin> read answer-defaults
ANSWER-DEFAULTS read

admin> set ppp-answer receive-auth = any-ppp-auth

admin> write
ANSWER-DEFAULTS written
```

With this setting, the system accepts session requests that provide any of the supported PPP authentication methods, but it drops requests that do not offer any authentication protocols during session negotiation.

Configuring bidirectional CHAP authentication

Bidirectional CHAP between the calling PPP device and the called PPP device increases compliance with the RFC 1994 standard for PPP CHAP authentication. Note

that the feature is not implemented for PAP-based authentication (PAP, PAP-Token, or PAP-Token-CHAP).

Note As noted in RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*, a security hole can occur when you use bidirectional authentication for an incoming call if the passwords used in both directions are identical. Bidirectional authentication in TAOS has been developed to avoid the security hole, even if the secrets are identical. For best results, however, Lucent recommends that you specify a different password for each authentication direction.

Overview of bidirectional CHAP settings

Bidirectional CHAP is supported locally and through RADIUS. For details about RADIUS settings, see the *TAOS RADIUS Guide and Reference*. Following are the relevant parameters, shown with default values:

```
[in ANSWER-DEFAULTS:ppp-answer]
bi-directional-auth = none
substitute-send-name = ""
[in CONNECTION/"":ppp-options]
substitute-recv-name = ""
recv-password = ""
send-password = ""
```

Parameter	Setting
`bi-directional-auth`	Whether CHAP authentication must be bidirectional. The default value of `none` disables bidirectional CHAP. If set to `allowed`, bidirectional CHAP is attempted. If the session request does not support it, the system does not reject the request, but if the second authentication pass fails, the session is terminated. If set to `required`, the system rejects a session request that does not perform bidirectional CHAP authentication, or that fails the second authentication pass.
`substitute-send-name`	System name to send to the far end for bidirectional CHAP authentication, if different from the `name` setting in the `system` profile.
`recv-password`	Password the system must receive from the calling device.
`send-password`	Password the system must send to the calling device during bidirectional CHAP.

Note When the `receive-auth-mode` parameter in the `answer-defaults` profile is set to `any-ppp-auth`, the system can accept both PAP and CHAP authentication. The `bi-directional-auth` setting is used only if a form of CHAP authentication has been negotiated. If any form of PAP authentication has been negotiated, the `bi-directional-auth` setting has no effect, even if set to `required`.

Allowing bidirectional CHAP for PPP session requests

The following commands make bidirectional CHAP the default authentication method attempted for PPP sessions requests:

```
admin> read answer-defaults
ANSWER-DEFAULTS read
admin> set profiles-required = yes
admin> set ppp-answer receive-auth-mode = any-ppp-auth
admin> set ppp-answer bidirectional-auth = allowed
admin> write
ANSWER-DEFAULTS written
```

With these settings, if a calling device accepts CHAP authentication, the system attempts to negotiate bidirectional CHAP, but does not reject the request if the negotiation fails. However, if bidirectional CHAP is negotiated, authentication must succeed in both directions. The following commands configure a `connection` profile that uses bidirectional CHAP:

```
admin> read connection subscriber-1
CONNECTION/subscriber-1 read
admin> set ip-options remote-address = 1.1.1.1/32
admin> set ppp-options bi-directional-auth = required
admin> set ppp-options send-auth-mode = chap-ppp-auth
admin> set ppp-options send-password = sendpw
admin> set ppp-options recv-password = recvpw
admin> write
CONNECTION/subscriber-1 written
```

Following is a comparable RADIUS user profile:

```
subscriber-1 Password = "recvpw"
     Service-Type = Framed,
     Ascend-Send-Secret = "sendpw",
     Framed-Protocol = PPP,
     Framed-IP-Address = 1.1.1.1,
     Framed-IP-Netmask = 255.255.255.255,
     Ascend-Route-IP = Route-IP-Yes
```

Token cards and dynamic passwords

The most secure password authentication uses token cards to overcome the limitations of static passwords. Token cards protect against both passive attacks and replay attacks, in which an unauthorized user records valid authentication information exchanged between systems and then replays it later to gain entry. Because token cards provide one-time-only passwords, the password changes many times a day, making replay impossible.

RADIUS is required for dynamic passwords using token cards. For details, see the *TAOS RADIUS Guide and Reference*.

Enabling the Link Quality Monitoring (LQM) protocol

The following parameter, shown with its default value, affects Link Quality Monitoring (LQM):

```
[in ANSWER-DEFAULTS:ppp-answer]
lqm = no
```

LQM enables the system to monitor data loss on a point-to-point link (see RFC 1989, *PPP Link Quality Monitoring*). The following set of commands enables LQM for all PPPoE clients that support the LQM protocol:

```
admin> read answer
ANSWER-DEFAULTS read

admin> set ppp-answer lqm = yes

admin> write
ANSWER-DEFAULTS written
```

Enabling LQM in the `answer-defaults` profile causes the system to send PPP echo requests to a PPP client (if LQM is negotiated with the client) and to detect if the client is offline while the DSL line and ATM are still active.

Specifying session time limits

After it authenticates a session request, the Stinger unit establishes a session and forwards the session's traffic to the IP router software. The system can use settings in the `answer-defaults` profile, or a `connection` or RADIUS profile, to apply filters or firewalls to the session's data stream and to time out the session if it becomes inactive for a specified time period.

Overview of profile settings

Following are some parameters for specifying session time limits and applying filters. The settings shown are the defaults.

```
[in ANSWER-DEFAULTS:session-info]
call-filter = ""
data-filter = ""
filter-persistence = no
idle-timer = 120
max-call-duration = 0

[in CONNECTION/"":session-options]
call-filter = ""
data-filter = ""
filter-persistence = no
idle-timer = 120
max-call-duration = 0

[in CONNECTION/"":telco-options]
call-type = off
```

Parameter	Setting
`call-filter`	Name of a call filter or firewall to apply. Call filters are used to exclude routine traffic from consideration when determining if a session is active or idle. For details, see the chapter on packet filters in the *Stinger T1000 Routing and Tunneling Supplement*.
`data-filter`	Name of a data filter or firewall to apply. Data filters are used for a variety of reasons, including network security. See the chapter on packet filters in the *Stinger T1000 Routing and Tunneling Supplement*.
`filter-persistence`	Enable/disable filter persistence across connection state changes. See the chapter on packet filters in the *Stinger T1000 Routing and Tunneling Supplement*.
`idle-timer`	Number of seconds a packetized network session can remain idle before it is terminated. The default value is 120.
`max-call-duration`	Maximum number of minutes a PPP session can stay connected.
`call-type`	Type of call. To enable the system to tear down inactive PPPoE sessions, leave the default `off` setting in the `connection` profile. To cause the system to keep the sessions running indefinitely, set to `ft1` for a nailed connection.

Time-limit settings in a RADIUS profile

RADIUS uses the following attribute-value pairs for setting session time limits:

RADIUS attribute	Value
Filter-ID (11)	Name of a `filter` profile. For details, see the chapter on packet filters in the *Stinger T1000 Routing and Tunneling Supplement*.
Idle-Timeout (28)	Maximum number of consecutive seconds of idle time allowed the user before termination of the session.
Session-Timeout (27)	Maximum number of seconds of service to be provided to the user before termination of the session.
Ascend-Maximum-Call-Duration (125)	Maximum number of minutes a call can stay connected.

Example of setting time limits

The following set of commands sets the idle timer to 60 seconds:

```
admin> read connection ppp-client
CONNECTION/ppp-client read
admin> set active = yes
admin> set encapsulation-protocol = ppp
```

```
admin> set ppp-options recv-password = localpw
admin> set ip-options remote-address = 1.1.1.1/24
admin> set telco-options call-type = off
admin> set session-options idle-timer = 60
admin> write
CONNECTION/ppp-client written
```

Following are comparable settings in a RADIUS profile:

```
ppp-client Password = "localpw"
   Service-Type = Framed-User,
   Framed-Protocol = PPP,
   Framed-IP-Address = 1.1.1.1,
   Framed-IP-Netmask = 255.255.255.0,
   Idle-Timeout = 60
```

Using session accounting

RADIUS enables administrators to keep track of connection statistics, usually for billing purposes. For details on session accounting attributes, see the *TAOS RADIUS Guide and Reference*.

Configuring PPP over Ethernet (PPPoE)

5

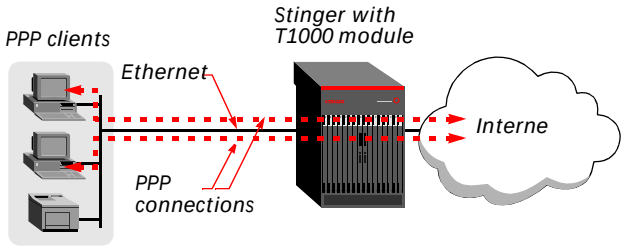
Introduction to PPPoE

With PPP over Ethernet (PPPoE), hosts on a shared Ethernet can initiate PPP sessions to multiple destinations through a single access device, which does not require IP routing support. The PPP connections use Ethernet-bridged framing, as defined in RFC 2516, *A Method for Transmitting PPP Over Ethernet (PPPoE)*.

PPPoE on a LAN interface

As shown in Figure 5-1, hosts on a local Ethernet can transmit PPP packets encapsulated in Ethernet-bridged frames to initiate a connection through the T1000 module.

Figure 5-1. Sample PPPoE topology



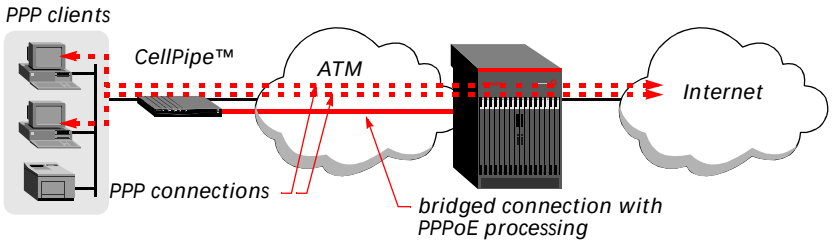
The T1000 module does not require LAN bridging to accept the PPPoE packets on the Ethernet interface. When it accepts the packets, the module begins a PPPoE negotiation phase, which is followed by a PPP negotiation phase. When the PPP session has been established, the packets are routed to the proper interface for egress.

Internet services can include Layer 2 Tunneling Protocol (L2TP) or Ascend Tunnel Management Protocol (ATMP), to tunnel to a remote virtual private network (VPN).

PPPoE on an ATM WAN interface

Figure 5-2 shows PPP clients on a shared remote Ethernet segment at customer premises.

Figure 5-2. Sample PPPoE topology across an ATM network



On the remote Ethernet, hosts send PPP packets encapsulated in Ethernet-bridged frames. The CellPipe™ unit transports the frames as a cell stream that uses AAL5 encapsulation as defined in RFC 1483, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*. When the Stinger unit receives the cell stream on the ATM WAN interface, it switches the cells to the T1000 internal interface on the basis of an ATM circuit configuration.

The T1000 module accepts the PPPoE packets when bridging is enabled on the WAN interface. After the PPPoE negotiation phase has been completed, a PPP negotiation phase starts. When the PPP session has been established, the packets are routed to the right (egress) interface.

Internet services can include L2TP or ATMP to tunnel to a remote VPN.

How PPPoE is negotiated on an ATM WAN interface

As described in RFC 2516, *A Method for Transmitting PPP Over Ethernet (PPPoE)*, PPPoE is negotiated in two phases: a discovery phase and a session phase. When a PC initiates a PPP session, the bridging CPE at that site initiates a PPPoE discovery phase in which the following events take place:

1 The bridging CPE sends a broadcast requesting availability of PPPoE services.

2 The T1000 module forwards the broadcast to a PPPoE server, either the onboard server in the module itself, or an external PPPoE server, depending on how the bridge profile is configured.

3 The PPPoE server responds with a packet that verifies its support for PPPoE and provides its media access controller (MAC) address.

4 The bridging CPE forwards the PPP session request from the PC client.

5 The PPPoE server responds with a unique session ID. Together, the MAC address and session ID uniquely identify the session.

When the client and the T1000 module have sufficient information, the PPP session phase begins. When the session has been established, the client sends PPP packets encapsulated in Ethernet-bridged frames.

Configuring PPPoE on WAN interfaces

Configuring PPPoE on a WAN interface such a DSL line requires the following configurations:

- An ATM circuit configuration between an ATM WAN interface and the T1000 internal interface. This configuration enables the system to forward the traffic stream received from the remote bridging device directly to the T1000 module. See "Configuring the ATM internal interface" on page 2-1.
- A permanent virtual circuit (PVC) configuration to the remote bridging device. This profile is sometimes referred to as the *bridge profile*. It must specify ATM encapsulation and packet bridging, and can also enable PPPoE.
- PPP client connection configurations, one for each PC that will establish a session through the remote bridging device. These profiles must specify PPP encapsulation, enable PPPoE, and specify the appropriate IP routing information.

Overview of bridge profile settings

In addition to the parameter settings used for typical terminating PVCs, all of which are described in the *Stinger ATM Configuration Guide*, the following additional parameters (shown with default values) apply for the PVC to a remote CPE bridge:

```
[in CONNECTION/"":bridging-options]
bridge = no
bridging-group = 0

[in CONNECTION/"":pppoe-options]
pppoe = no
bridge-non-pppoe = no

[in CONNECTION/"":atm-options]
atm-circuit-profile = ""
```

Parameter	Setting
`bridge`	Enable/disable packet bridging on the interface. Set to `yes` in the bridge profile. For details, see Chapter 3, "Configuring Packet Routing and Bridging."
`bridging-group`	Group number, from 0 to 65535. A nonzero `bridging-group` setting is recommended for performance reasons in the bridge profile. For details about bridging groups, see Chapter 3, "Configuring Packet Routing and Bridging."
`pppoe`	Enable/disable processing of PPPoE packets. When set to `yes`, PPPoE requests received from the bridging device are handled by the onboard PPPoE server in the T1000 module. If PPPoE is not enabled on an interface, the T1000 module bridges the PPPoE requests to an external PPPoE server.
`bridge-non-pppoe`	Enable/disable bridging of packets other than PPPoE. With the default `no` value, the T1000 module bridges only PPPoE packets and discards other types of bridged packets.

Parameter	Setting
`atm-circuit-profile`	Text name of the `connection` profile that defines the ATM circuit between the ATM WAN interface used to reach the bridging CPE and the T1000 internal interface. See "Configuring the ATM internal interface" on page 2-1 for details.

RADIUS uses the following attribute-value pairs for a bridged connection to the remote CPE:

RADIUS attribute	Setting
Ascend-Bridge (230)	Enable/disable packet bridging on the interface. Set to Bridge-Yes (1) in the bridge profile. For details, see Chapter 3, "Configuring Packet Routing and Bridging."
Ascend-BIR-Bridge-Group (7)	Group number, from 0 to 65535. A nonzero `bridging-group` setting is recommended for performance reasons in the bridge profile. For details about bridging groups, see Chapter 3, "Configuring Packet Routing and Bridging."
Ascend-PPPoE-Enable (74)	Enable/disable processing of PPPoE packets. With a value of PPPoE-Yes (1), PPPoE packets flow to the PPPoE server in the T1000 module, and then the PPPoE discovery and PPP session negotiation occur inside the Stinger unit. With a value of PPPoE-No (2) in the bridge profile, then the T1000 module does not recognize PPPoE packets and bridges them to an external PPPoE server.
Ascend-Bridge-Non-PPPoE (75)	Enable/disable bridging of packets other than PPPoE for the user profile. Valid values are Bridge-Non-PPPoE-No (0) and Bridge-Non-PPPoE-Yes (1).
Ascend-ATM-Circuit-Name (262)	Text user name of the profile that defines the ATM circuit between the WAN interface used to reach the remote bridging CPE, and the T1000 module. See "Bridge profile to the CPE" on page 5-7 for an example.

Overview of PPP client profile settings

Each PPP client requires a `connection` or RADIUS profile that uses PPP encapsulation and IP routing, and enables PPPoE. For information about configuring IP routing and tunneling options, see the *Stinger T1000 Routing and Tunneling Supplement*. Following is a minimal subset of the relevant parameters, shown with default settings:

```
[in CONNECTION/""]
station* = ""
encapsulation-protocol = atm

[in CONNECTION/"":ip-options]
ip-routing-enabled = yes
remote-address = 0.0.0.0/0
```

```
[in CONNECTION/"":ppp-options]
recv-password = ""
```

Parameter	Setting
`station`	Name of the PPP client. The value is case sensitive, and must exactly match the name the client presents during authentication.
`encapsulation-protocol`	Encapsulation protocol. Set to `ppp` for PPP clients.
`ip-routing-enabled`	Enable/disable IP routing for the interface. IP routing is enabled by default.
`remote-address`	IP address of the remote device, which can include a subnet specification. If the address does not include a subnet mask, the router assumes the default mask based on address class.
`recv-password`	Password expected from the caller.

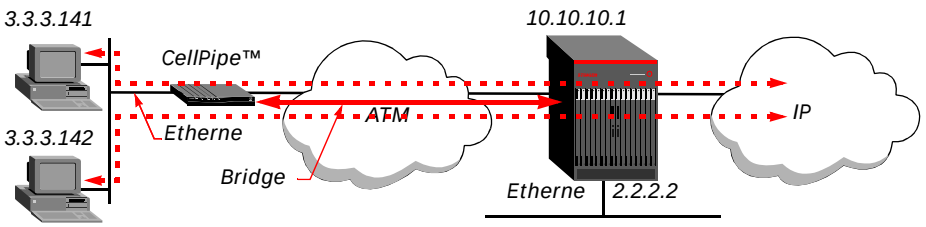
RADIUS uses the following attribute-value pairs for PPPoE connections:

RADIUS attribute	Setting
Password (2)	Password expected from the caller for a dial-in connection.
Service-Type (6)	Type of services the link can use. Set to Framed for PPP sessions.
Framed-Protocol (7)	Encapsulation protocol. Set to PPP (1) for PPPoE.
Ascend-Route-IP (228)	Enable/disable IP routing for the interface. IP routing is enabled by default.
Framed-IP-Address (8)	IP address of the calling device.
Framed-IP-Netmask (9)	Subnet mask of the caller's address. If you do not specify a subnet mask, the router assumes the default mask based on address class.

Typical PPPoE configuration across an ATM interface

In Figure 5-3, a DSL CellPipe™ unit operating as a bridge is connected to an Ethernet that supports two PCs with PPP software.

Figure 5-3. Example of PPPoE across an ATM WAN interface



This sample configuration shows how to create the profiles required to enable the two PCs in Figure 5-3 to establish PPP sessions through the Stinger unit to the IP cloud beyond it.

ATM circuit between the ATM WAN and T1000 internal interface

The following commands determine the nailed-group number of the first SDSL interface in slot 5:

```
admin> which -n { 1 5 1 }
Nailed group corresponding to port { shelf-1 slot-5 1 } is 201
```

The following commands determine the nailed-group number of the internal interface of a T1000 module in slot 3:

```
admin> get atm-internal { 1 3 1 } line-config nailed-group
[in ATM-INTERNAL/{ shelf-1 slot-3 1 }:line-config:nailed-group]
nailed-group = 101
```

The following commands configure an ATM circuit between the first SDSL interface in slot 5 and the T1000 internal interface:

```
admin> new connection sdsl-t1000
CONNECTION/sdsl-t1000 read

admin> set active = yes

admin> set encapsulation-protocol = atm-circuit

admin> set ip-options ip-routing = no

admin> set atm-options vpi = 0

admin> set atm-options vci = 35

admin> set atm-options nailed-group = 201

admin> set atm-connect-options vpi = 0

admin> set atm-connect-options vci = 35

admin> set atm-connect-options nailed-group = 101

admin> write
CONNECTION/sdsl-t1000 written
```

Following is a comparable RADIUS profile:

```
permconn-st-1 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-CIR,
    User-Name = "sdsl-t1000",
    Ascend-ATM-Group = 201,
    Ascend-Route-IP = Route-IP-No,
    Ascend-ATM-Vpi = 0,
    Ascend-ATM-Vci = 35,
    Ascend-ATM-Connect-Vpi = 0,
    Ascend-ATM-Connect-Vci = 35,
    Ascend-ATM-Connect-Group = 101
```

For background information about circuit configurations, see the *Stinger ATM Configuration Guide*.

Bridge profile to the CPE

For performance reasons, specifying a unique `bridging-group` value on a PPPoE interface is recommended. A unique group guarantees that packets will not flow between two bridge interfaces. The following commands configure a bridge profile to the remote CPE with PPPoE enabled:

```
admin> new connection t1000-bridge
CONNECTION/t1000-bridge read
admin> set active = yes
admin> set encapsulation-protocol = atm
admin> set ip-options ip-routing = no
admin> set bridging-options bridging-group = 1
admin> set bridging-options bridge = yes
admin> set pppoe-options pppoe = yes
admin> set atm-options vpi = 0
admin> set atm-options vci = 36
admin> set atm-options nailed-group = 101
admin> set atm-options atm-circuit-profile = sdsl-t1000
admin> write
CONNECTION/t1000-bridge written
```

Note The `atm-circuit-profile` setting specifies the name of the profile in which the ATM circuit is configured.

Following is a comparable RADIUS profile:

```
permconn-st-2 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-1483,
    User-Name = "t1000-bridge",
    Ascend-ATM-Group = 101,
    Ascend-Route-IP = Route-IP-No,
    Ascend-ATM-Vpi = 0,
    Ascend-ATM-Vci = 36,
    Ascend-Bridge = Bridge-Yes,
    Ascend-PPPoE-Enable = Ascend-PPPoE-Enable,
    Ascend-ATM-Circuit-Name = sdsl-t1000
```

PPP client connections with IP routing

For background information about configuring IP routed connections, see the *Stinger T1000 Routing and Tunneling Supplement*. The following commands configure a `connection` profile for the first PPP client:

```
admin> new connection ppp-1
CONNECTION/ppp-1 read
admin> set active = yes
admin> set encapsulation-protocol = ppp
admin> set ip-options remote-address = 3.3.3.141/29
admin> set ppp-options recv-password = ppp-1!pw
```

```
admin> write
CONNECTION/ppp-1 written
```

The following commands modify the preceding connection profile to create a new profile for the second PPP client:

```
admin> set station = ppp-2
(New index value; will save as new profile CONNECTION/ppp-2.)
admin> set ip-options remote-address = 3.3.3.142/29
admin> set ppp-options recv-password = ppp-2!pw
admin> write
CONNECTION/ppp-2 written
```

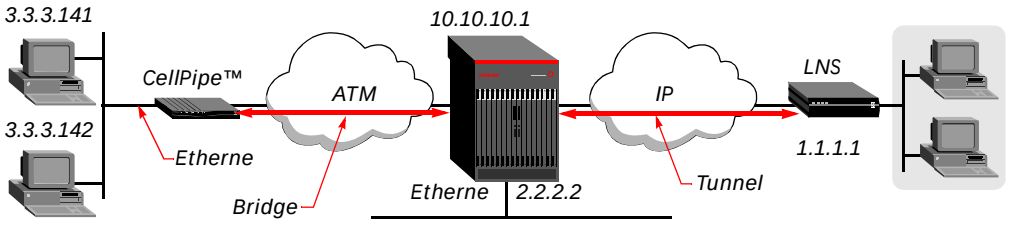
Following are comparable RADIUS user profiles:

```
ppp-1 Password = "ppp-1!pw"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Framed-IP-Address = 3.3.3.141,
    Framed-IP-Netmask = 255.255.255.248
ppp-2 Password = "ppp-2!pw"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Framed-IP-Address = 3.3.3.142,
    Framed-IP-Netmask = 255.255.255.248
```

Example of PPPoE that includes a tunnel to a remote VPN

Figure 5-4 shows the PPP clients configured in the preceding example, and adds an L2TP network server (LNS) that provides virtual private network (VPN) access to a remote site.

Figure 5-4. Example of PPP sessions that include L2TP tunneling



For background information about tunneling protocol configurations, see the *Stinger T1000 Routing and Tunneling Supplement*. The following commands configure L2TP connectivity to the remote LNS:

```
admin> read l2-tunnel-global
L2-TUNNEL-GLOBAL read
admin> set l2tp-mode = lac
admin> set l2tp-auth-enabled = yes
admin> set l2tp-system-name = stinger-1
admin> write
L2-TUNNEL-GLOBAL written
```

```
admin> read tunnel-server lns-1
TUNNEL-SERVER/1.1.1. read
admin> set shared-secret = !value!
admin> write
TUNNEL-SERVER/1.1.1.1 written
```

The following commands modify the PPP connection profiles configured in "PPP client connections with IP routing" on page 5-7, to route their traffic stream across the IP cloud to an LNS:

```
admin> read connection ppp-1
CONNECTION/ppp-1 read
admin> set tunnel-options profile-type = mobile-client
admin> set tunnel-options tunneling-protocol = l2tp-protocol
admin> set tunnel-options primary-tunnel-server = 1.1.1.1
admin> write
CONNECTION/ppp-1 written
admin> read connection ppp-2
CONNECTION/ppp-2 read
admin> set tunnel-options profile-type = mobile-client
admin> set tunnel-options tunneling-protocol = l2tp-protocol
admin> set tunnel-options primary-tunnel-server = 1.1.1.1
admin> write
CONNECTION/ppp-2 written
```

Configuring PPPoE on a LAN interface

To support PPPoE on a LAN interface, the ethernet profile for the T1000 Ethernet interface must enable PPPoE. You can then configure connections for each LAN PPP client.

Note The PPP client profile settings are the same whether the client resides on a local or WAN interface. For an overview of the client settings, see "Overview of PPP client profile settings" on page 5-4.

Overview of Ethernet profile settings for local PPPoE

Following are the parameters, shown with default values, for enabling PPPoE on a T1000 Ethernet interface:

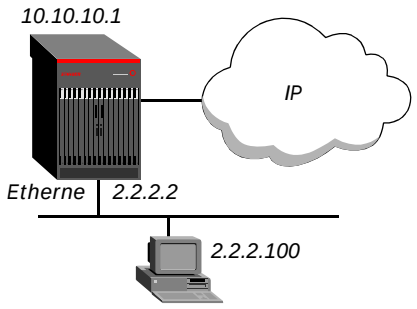
```
[in ETHERNET/{ any-shelf any-slot 0 }:pppoe-options]
pppoe = no
bridge-non-pppoe = no
```

Parameter	Setting
pppoe	Enable/disable processing of PPPoE packets. When set to yes, PPPoE requests received on the interface are handled by the onboard PPPoE server in the T1000 module. If PPPoE is not enabled on an interface and bridging is enabled, the T1000 module bridges the PPPoE requests to an external PPPoE server. If both PPPoE and packet bridging are disabled on the Ethernet interface, PPPoE packets will be discarded. Under those conditions, only IP packets will be accepted on the interface.
bridge-non-pppoe	Enable/disable bridging of packets other than PPPoE when LAN bridging is enabled on the Ethernet interface. With the default no value, the system bridges only PPPoE packets and discards all other types of bridged packets. This setting does not apply unless bridging is enabled on the interface.

Typical PPPoE configuration on a LAN interface

Figure 5-5 shows a PC on an IP network on a T1000 Ethernet interface.

Figure 5-5. Example of PPPoE on a LAN interface



The following commands configure the ethernet profile and its IP interface:

```
admin> read ethernet { 1 3 1 }
ETHERNET/{ shelf-1 slot-3 1 } read
admin> set bridging-options bridging-group = 2
admin> set pppoe-options pppoe = yes
admin> write
ETHERNET/{ shelf-1 slot-3 1 } written
admin> read ip-interface { { 1 3 1 } 0}
IP-INTERFACE/{ { shelf-1 slot-3 1 } 0 } read
admin> set ip-address = 2.2.2.2/28
admin> write
IP-INTERFACE/{ { shelf-1 slot-3 1 } 0 } written
```

The following commands define a connection profile for the local client in Figure 5-5:

```
admin> new connection ppp-3
CONNECTION/ppp-3 read
admin> set active = yes
admin> set encapsulation-protocol = ppp
admin> set ip-options remote-address = 2.2.2.100/28
admin> set ppp-options recv-password = ppp-3!pw
admin> write
CONNECTION/ppp-3 written
```

Following is a comparable RADIUS profile for the local client:

```
pppoe3 Password = "ppp-3!pw"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Framed-IP-Address = 2.2.2.100,
    Framed-IP-Netmask = 255.255.255.240
```

Multilink PPP (MP) connections

Multilink PPP (MP) uses the encapsulation defined in RFC 1990. MP enables a client to use a static number of channels. Both sides of the connection must support MP encapsulation.

PPP `answer-defaults` and `connection` profile settings also apply to MP connections. If you configure an MP connection on a Stinger unit that cannot successfully negotiate the connection, the unit falls back to single-channel PPP.

Note For optimum performance, both sides of a connection must set the `base-channel-count` parameter to the same value.

Settings in a Connection profile

Following are the parameters related to MP connections, shown here with default setting.

```
[in CONNECTION/""]
encapsulation-protocol = mpp
[in CONNECTION/"":mp-options
base-channel-count = 1
minimum-channels = 1
maximum-channels = 2
```

Parameter	Setting
`encapsulation-protocol`	Encapsulation protocol. Set this parameter to `mp` for Multilink PPP connections.
`base-channel-count`	Base number of channels to use for a multilink PPP connection. When a call is received, the Stinger unit authenticates the first (base) channels of the call and then determines the maximum and minimum settings.

Parameter	Setting
`minimum-channels`	Minimum number of channels available to a multilink PPP connection. In the current software version, the value can apply to Multilink Protocol Plus™ (MP+) but not MP connections.
`maximum-channels`	Maximum number of channels available to a multilink PPP connection. In the current software version, the value can apply to MP+ but not MP connections.

Settings in a RADIUS profile

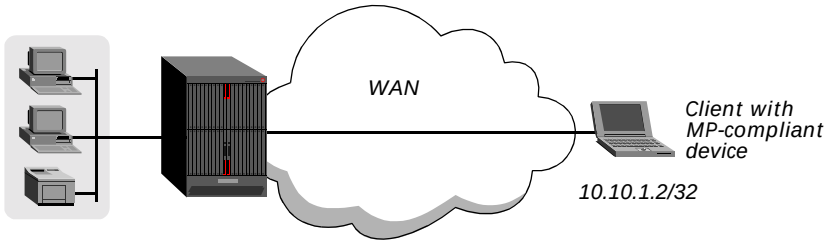
RADIUS uses the following attribute-value pairs for dial-in MP connections:

RADIUS attribute	Value
Framed-Protocol (7)	Encapsulation protocol. MP (262) indicates Multilink Protocol.
Ascend-Base-Channel-Count (172)	Base number of channels to use for a multilink PPP connection. When a call is received, the Stinger unit authenticates the first (base) channels of the call and then determines the maximum and minimum settings.
Ascend-Minimum-Channels (173)	Minimum number of channels available to a multilink PPP connection. In the current software version, the value can apply to MP+ but not MP connections.
Ascend-Maximum-Channels (235)	Maximum number of channels available to a multilink PPP connection. In the current software version, the value can apply to MP+ but not MP connections. **Note** If a RADIUS profile does not specify Ascend-Maximum-Channels, the default value of 1 prevents the client from establishing a multichannel call.

Examples of an MP connection

The MP connection shown in Figure 5-6 is allocated two channels.

Figure 5-6. Multilink PPP (MP) connection



Following are the commands entered to configure a local profile, and the system's responses:

```
admin> new connection kory
CONNECTION/kory read
admin> set active = yes
```

```
admin> set encapsulation-protocol = mp
admin> set ip remote-address = 10.10.1.2/32
admin> set ppp recv-password = localpw
admin> set mp base-channel-count = 2
admin> write
CONNECTION/kory written
```

Following is a comparable RADIUS profile:

```
kory Password = "localpw"
   Service-Type = Framed-User,
   Framed-Protocol = MP,
   Framed-IP-Address = 10.10.1.2,
   Framed-IP-Netmask = 255.255.255.255,
   Ascend-Base-Channel-Count = 2,
   Ascend-Maximum-Channels = 2
```

MP bonding of analog calls

MP also operates on modem cards to bond multiple channels for analog calls. This feature enables a client with two modems to connect to the unit at a speed that is the aggregate speed of both connections. For example, a Windows NT 4.0 system with two 56Kbps modems, and Dial Up Networking (DUN) configured to use multiple lines, can set both modems to dial in to a Stinger unit.

Note Some client modems and software packages have compatibility problems with MP channel bonding.

To enable MP bonding of analog calls, specify a standard MP connection. For example:

```
admin> new connection baskar
CONNECTION/baskar read
admin> set active = yes
admin> set encapsulation-protocol = mp
admin> set ip remote-address = 10.10.1.2/29
admin> set ppp recv-password = localpw
admin> set mp base-channel-count = 2
admin> write
CONNECTION/baskar written
```

Or, in a RADIUS profile:

```
baskar Password = "localpw"
   Service-Type = Framed-User,
   Framed-Protocol = MP,
   Framed-IP-Address = 10.10.1.2,
   Framed-IP-Netmask = 255.255.255.248,
   Ascend-Base-Channel-Count = 2
```

The first 56Kbps modem call negotiates the MP connection, and the second modem call is bundled with the first. The Stinger unit reports a single MP user with a 128Kbps connection.

Multilink Protocol Plus (MP+) connections

Multilink™ Protocol Plus (MP+) uses PPP encapsulation with TAOS extensions, as described in RFC 1934. MP+ enables a Stinger unit to monitor traffic on a connection with another Stinger unit and add or subtract bandwidth on demand. The criteria for adding or dropping bandwidth are part of the TAOS extensions, and are supported only by Lucent Technologies equipment.

On MP+ connections, the side that makes the first call makes all subsequent calls to add bandwidth. If a remote user or access router dials in, all calls dialed to add channels are also dialed in. If the Stinger unit initiates the first call, all calls to add channels are dialed out.

PPP and MP `answer-defaults` and `connection` profile settings also apply to MP+ connections. To specify the base channels of an MP+ connection, you must configure the `mp-options` subprofile, as described in "Multilink PPP (MP) connections" on page 5-11.

Settings in a Connection profile

Following are the `connection` profile parameters related to MP+ connections. The settings shown are the defaults.

```
[in CONNECTION/""]
encapsulation-protocol = mpp
```

```
[in CONNECTION/"":mpp-options]
aux-send-password = ""
dynamic-algorithm = quadratic
bandwidth-monitor-direction = transmit
increment-channel-count = 1
decrement-channel-count = 1
seconds-history = 15
add-persistence = 5
sub-persistence = 10
target-utilization = 70
```

Parameter	Setting
`encapsulation-protocol`	Encapsulation protocol. The default value `mpp` specifies MP+. The far end must be a TAOS unit.
`aux-send-password`	Password the Stinger unit sends when it adds channels to an MP+ call that uses PAP-Token-CHAP authentication.
`dynamic-algorithm`	Algorithm for calculating average line utilization (ALU) over a certain number of seconds (`seconds-history`).
`bandwidth-monitor-direction`	Direction in which criteria for adding or dropping links apply. Set to `transmit` to monitor traffic sent across the link, `transmit-recv` to monitor traffic sent and received, or `none` to turn off link utilization monitoring. If both sides of the link have `bandwidth-monitor-direction` set to `none`, Dynamic Bandwidth Allocation (DBA) protocol is disabled.
`increment-channel-count`	Number of channels the Stinger unit can add at one time, subject to the setting of the `parallel-dialing` parameter in the `system` profile.

Parameter	Setting
`decrement-channel-count`	Number of channels the Stinger unit can subtract at one time, dropping the newest channels first.
`seconds-history`	Number of seconds to use as the basis for calculating average line utilization (ALU).
`add-persistence`	Number of seconds for which ALU must persist beyond the `target-utilization` threshold before the Stinger unit adds bandwidth.
`sub-persistence`	Number of seconds for which the ALU must persist below the `target-utilization` threshold before the unit subtracts bandwidth.
`target-utilization`	Percentage of line utilization (the default setting is 70%) to use as a threshold when determining when to add or subtract bandwidth.

Settings in a RADIUS profile

A RADIUS user profile can specify the following attributes for configuring a MP+ connection's PPP options, in addition to the MP parameters described in "Multilink PPP (MP) connections" on page 5-11:

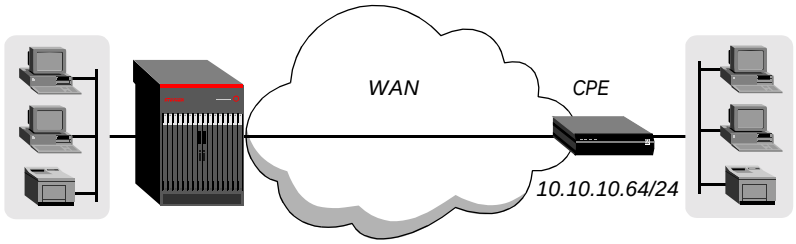
RADIUS attribute	Value
Framed-Protocol (7)	Encapsulation protocol. MPP (256) indicates an MP+ connection with another TAOS unit.
Ascend-History-Weigh-Type (239)	Algorithm for calculating average line utilization (ALU) over a certain number of seconds.
Ascend-DBA-Monitor (171)	Criteria for adding or subtracting bandwidth from the connection. You can specify DBA-Transmit (0), DBA-Transmit-Recv (1), or DBA-None (3). If both sides of the link have Bandwidth-Monitor-Direction set to None, DBA is disabled.
Ascend-Inc-Channel-Count (236)	Number of channels the Stinger unit can add at one time, subject to the setting of the `parallel-dialing` parameter in the `system` profile.
Ascend-Dec-Channel-Count (237)	Number of channels the Stinger unit can subtract at one time, dropping the newest channels first.
Ascend-Seconds-Of-History (238)	Number of seconds to use as the basis for calculating average line utilization (ALU).
Ascend-Add-Seconds (240)	Number of seconds for which ALU must persist beyond the Target-Utilization threshold before the Stinger unit adds bandwidth.
Ascend-Remove-Seconds (241)	Number of seconds for which the ALU must persist below the Target-Utilization threshold before the unit subtracts bandwidth.
Ascend-Target-Util (234)	Percentage of line utilization (default 70%) to use as a threshold when determining when to add or subtract bandwidth.

RADIUS attribute	Value
Ascend-Maximum-Channels (235)	Maximum number of channels available to a multilink PPP connection. In the current software version, the value can apply to MP+ but not MP connections. **Note** If a RADIUS profile does not specify Ascend-Maximum-Channels, the default value of 1 prevents the client from establishing a multichannel call.

Example of an MP+ configuration

In Figure 5-7, the Stinger unit and the CPE are configured for MP+.

Figure 5-7. Multilink™ Protocol Plus (MP+) connection



The following commands create a `connection` profile for the far-end CPE unit:

```
admin> new connection pipe1
CONNECTION/pipe1 read

admin> set active = yes

admin> set encapsulation-protocol = mpp

admin> set ip remote-address = 10.10.10.64/24

admin> set ppp recv-password = localpw

admin> set mp base-channel-count = 2

admin> set mpp bandwidth-monitor-direction = transmit-recv

admin> set mpp seconds-history = 30

admin> set mpp add-persistence = 10

admin> write
CONNECTION/pipe1 written
```

Following is a comparable RADIUS profile:

```
pipe1 Password = "localpw"
   Service-Type = Framed-User,
   Framed-Protocol = MPP,
   Framed-IP-Address = 10.10.10.64,
   Framed-IP-Netmask = 255.255.255.0,
   Ascend-Base-Channel-Count = 2,
   Ascend-Maximum-Channels = 2,
   Ascend-DBA-Monitor = DBA-Transmit-Recv,
```

```
Ascend-Seconds-Of-History = 30,
Ascend-Add-Seconds = 10
```

Note The RADIUS profile must specify Ascend-Maximum-Channels, or the default value of 1 prevents the client from establishing a multichannel call.

Configuring PPP over ATM (PPPoA)

6

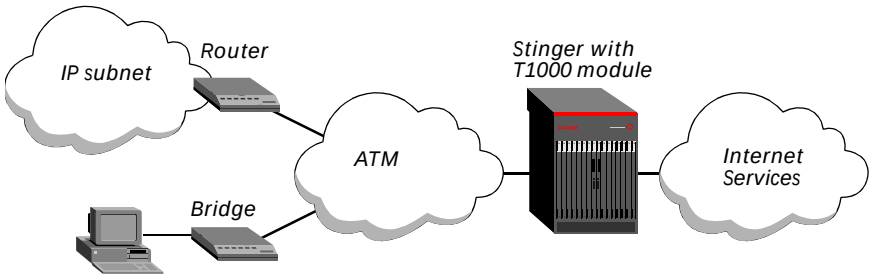
Introduction to PPPoA

PPP can use the ATM adaptation layer 5 (AAL5) protocol as a framing mechanism across point-to-point virtual circuits, as described in RFC 2364, *PPP over AAL5*. This capability is referred to as PPP over ATM (PPPoA).

PPPoA clients often have an assigned IP host address. However, if the CPE connecting the client to the ATM core network is a bridging modem rather than an IP router, the Stinger unit can forward the connection's traffic stream on the basis of packet bridging alone, or bridged IP routing (BIR). For background on these bridging operations, see Chapter 3, "Configuring Packet Routing and Bridging."

Figure 6-1 shows PPPoA clients accessing a Stinger unit.

Figure 6-1. Sample PPPoA topology



PPPoA clients transmit PPP packets encapsulated in AAL5. The Stinger unit switches the cells to the T1000 internal interface on the basis of an ATM circuit configuration, and uses IP routing to forward the packet streams to the appropriate egress interface.

Internet services can include L2TP or ATMP to tunnel to a remote VPN. With the current software version, the following limitations apply:

- Only VC-multiplexed PPPoA is currently supported.
- Only incoming PPPoA connections are currently supported.

Configuring PPPoA with IP routing

To enable establishment of a PPPoA client connection using IP routing, the following configurations are required:

- An ATM circuit between the ATM WAN interface and the T1000 internal interface. This configuration enables the system to switch the traffic stream received from the remote host directly to the T1000. See "Configuring the ATM internal interface" on page 2-1.
- PPPoA client connection configurations, one for each client. These profiles must specify PPP encapsulation and must also specify the appropriate IP routing information. These profiles do not need to use the `atm-circuit-profile` parameter to reference a specific circuit profile.

Overview of IP-routed PPPoA client profile settings

Each PPPoA client requires a `connection` or RADIUS profile. These profiles must specify PPP encapsulation and must also specify the appropriate IP routing information. For background information about IP routing options, tunneling options, and other IP-related configurations you can specify for a client session, see the *Stinger T1000 Routing and Tunneling Supplement*. Following is a minimal subset of the relevant parameters, shown with default settings:

```
[in CONNECTION/""]
station* = ""
encapsulation-protocol = atm

[in CONNECTION/"":ip-options]
ip-routing-enabled = yes
remote-address = 0.0.0.0/0

[in CONNECTION/"":ppp-options]
recv-password = ""
```

Parameter	Setting
`station`	Name of the PPPoA client. The value is case sensitive, and must exactly match the name the client presents during authentication.
`encapsulation-protocol`	Encapsulation protocol. Set to `ppp` for PPPoA clients.
`ip-routing-enabled`	Enable/disable IP routing for the interface. IP routing is enabled by default.
`remote-address`	IP address of the remote device, which can include a subnet specification. If the address does not include a subnet mask, the router assumes the default subnet mask based on address class.
`recv-password`	Password expected from the caller.

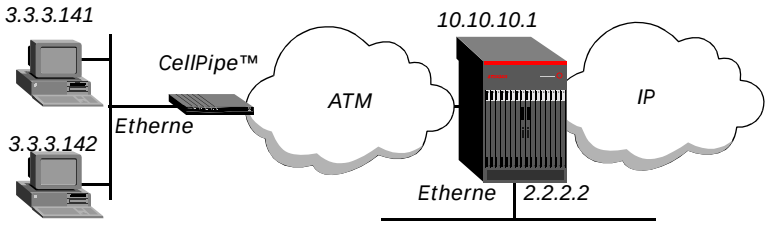
RADIUS uses the following attribute-value pairs for PPPoA connections:

RADIUS attribute	Setting
Password (2)	Password expected from the caller for a dial-in connection.
Service-Type (6)	Type of services the link can use. Set to Framed for PPPoA sessions.
Framed-Protocol (7)	Encapsulation protocol. Set to PPP (1) for PPPoA.
Ascend-Route-IP (228)	Enable/disable IP routing for the interface. IP routing is enabled by default.
Framed-IP-Address (8)	IP address of the calling device.
Framed-IP-Netmask (9)	Subnet mask of the caller's address. If you do not specify a subnet mask, the router assumes the default subnet mask based on address class.

Typical PPPoA configuration for routed clients

Figure 6-2 shows a Stinger unit with a T1000 module installed. Across an SDSL interface, a CellPipe™ unit is operating as a router with an IP subnet that supports two PCs with PPP client software.

Figure 6-2. Example of subnet of PPP clients accessing a Stinger over ATM



This sample configuration shows how to create the profiles required to enable the two PCs in Figure 6-2 to establish PPP sessions through the Stinger unit to the IP cloud beyond it. For background information about ATM circuit configurations, see the *Stinger ATM Configuration Guide*.

ATM circuit configuration

The following commands determine the nailed-group number of the first SDSL interface in slot 5:

```
admin> which -n { 1 5 1 }
Nailed group corresponding to port { shelf-1 slot-5 1 } is 201
```

The following commands determine the nailed-group number of the internal interface of a T1000 module in slot 3:

```
admin> get atm-internal { 1 3 1 } line-config nailed-group
[in ATM-INTERNAL/{ shelf-1 slot-3 1 }:line-config:nailed-group]
nailed-group = 101
```

The following commands configure a connection profile for an ATM circuit between the SDSL interface and the T1000 internal interface:

```
admin> new connection sdsl-t1000
CONNECTION/sdsl-t1000 read
admin> set active = yes
admin> set encapsulation-protocol = atm-circuit
admin> set ip-options ip-routing = no
admin> set atm-options vpi = 0
admin> set atm-options vci = 35
admin> set atm-options nailed-group = 201
admin> set atm-connect-options vpi = 0
admin> set atm-connect-options vci = 35
admin> set atm-connect-options nailed-group = 101
admin> write
CONNECTION/sdsl-t1000 written
```

Following is a comparable RADIUS profile:

```
permconn-st-1 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-CIR,
    User-Name = "sdsl-t1000",
    Ascend-ATM-Group = 201,
    Ascend-Route-IP = Route-IP-No,
    Ascend-ATM-Vpi = 0,
    Ascend-ATM-Vci = 35,
    Ascend-ATM-Connect-Vpi = 0,
    Ascend-ATM-Connect-Vci = 35,
    Ascend-ATM-Connect-Group = 101
```

PPPoA client connections with IP routing

For background information about configuring IP routed connections, see the *Stinger T1000 Routing and Tunneling Supplement*. The following commands configure connection profiles for two PPPoA clients:

```
admin> new connection pppoa1
CONNECTION/pppoa1 read
admin> set active = yes
admin> set encapsulation-protocol = ppp
admin> set ip-options remote-address = 3.3.3.141/29
admin> set ppp-options recv-password = ppp1!pw
admin> write
CONNECTION/pppoa1 written
admin> set station = pppoa2
(New index value; will save as new profile CONNECTION/pppoa2.)
admin> set ip-options remote-address = 3.3.3.142/29
admin> set ppp-options recv-password = ppp2!pw
```

```
admin> write
CONNECTION/pppoa2 written
```

Following are comparable RADIUS user profiles:

```
pppoa1 Password = "ppp1!pw"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Framed-IP-Address = 3.3.3.141,
    Framed-IP-Netmask = 255.255.255.248
pppoa2 Password = "ppp2!pw"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Framed-IP-Address = 3.3.3.142,
    Framed-IP-Netmask = 255.255.255.248
```

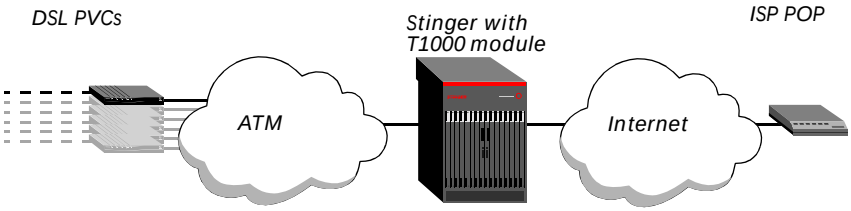
Configuring RFC 1483 PVC Aggregation

7

Introduction

RFC 1483, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*, defines a method for transporting packets across an ATM backbone without requiring multihop routes through the ATM cloud. With a T1000 module installed, you can use IP routing to aggregate many RFC 1483 PVCs from DSL subscribers onto a single virtual circuit to a specific IP destination such as an ISP. This capability, illustrated in Figure 7-1, greatly simplifies provisioning new DSL subscribers that are routed to an ISP.

Figure 7-1. Aggregating subscriber PVCs onto a single virtual circuit using IP routing



Internet services can include L2TP or ATMP tunneling to a remote VPN.

Configuring RFC 1483 routed connections

Aggregating RFC 1483 PVCs requires the following configurations:

- An ATM circuit between each subscriber ATM WAN interface and the T1000 internal interface. This configuration enables the system to switch the traffic stream received from the subscriber directly to the T1000 module. See “Configuring the ATM internal interface” on page 2-1.
- A terminating PVC configuration to the remote ISP.

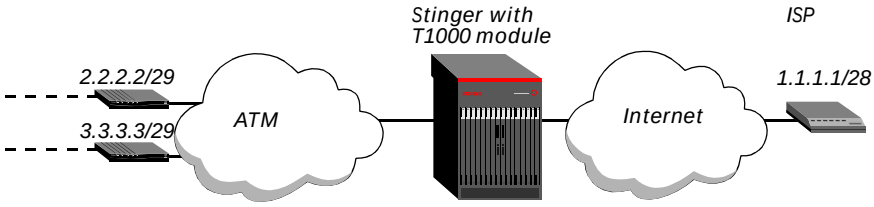
Where to find details about ATM connection settings

For background information about both ATM circuit and terminating ATM connections, see the *Stinger ATM Configuration Guide*. This guide shows how to use these standard ATM configurations to enable the T1000 to use routing for PVC aggregation.

Example of PVC aggregation using IP routing

In the example shown in Figure 7-2, two IP-routed DSL subscriber connections log into the same ISP across the Internet. The Stinger unit receives the IP connections over ATM, terminates them on the T1000 module, and routes the multiple connections to the ISP across the same virtual circuit.

Figure 7-2. Multiple DSL connections routed to the same ISP



This sample configuration shows how to create the Stinger profiles required to enable the two PCs in Figure 7-2 to establish an IP connection to their ISP.

Note The VPI-VCI pair must be different in the two subscriber profiles. In addition, there is a limitation on the number of `connection` profiles the system can enable on the T1000. Of the range of approximately 2,000 VPI-VCI pairs allocated to the LIM, the T1000 can use only 1,000.

Identifying the ATM interface nailed-group numbers

In the example configurations, the subscriber connections use the first and second ports of an SDSL module installed in slot 5, and the T1000 module is installed in slot 3. For example:

```
admin> show
Controller { first-control-module } ( PRIMARY ):
                                Reqd  Oper  Slot Type
  { second-control-module }     UP    DOWN  ( SECONDARY )
  { shelf-1 slot-2 0 }          UP    UP    dadsl-atm-24-card
  { shelf-1 slot-3 0 }          UP    UP    terminator-card
  { shelf-1 slot-5 0 }          UP    UP    sdsl-atm-v2-card
  { shelf-1 trunk-module-1 0 } UP    UP    ds3-atm-trunk-daughter-card
  { shelf-1 trunk-module-2 0 } UP     UP    oc3-atm-trunk-daughter-card
```

The following commands determine the nailed-group number of the first and second SDSL interfaces in slot 5:

```
admin> which -n { 1 5 1 }
Nailed group corresponding to port { shelf-1 slot-5 1 } is 201

admin> which -n { 1 5 2 }
Nailed group corresponding to port { shelf-1 slot-5 1 } is 202
```

The following commands determine the nailed-group number of the internal interface of a T1000 module in slot 3:

```
admin> get atm-internal { 1 3 1 } line-config nailed-group
[in ATM-INTERNAL/{ shelf-1 slot-3 1 }:line-config:nailed-group]
nailed-group = 101
```

Defining the first PVC to be routed to the ISP

The following commands configure an ATM circuit between the first SDSL interface and the T1000 internal interface:

```
admin> new connection sdsl1-t1000
CONNECTION/sdsl1-t1000 read
admin> set active = yes
admin> set encapsulation-protocol = atm-circuit
admin> set ip-options ip-routing = no
admin> set atm-options vpi = 8
admin> set atm-options nailed-group = 201
admin> set atm-connect-options vpi = 1
admin> set atm-connect-options vci = 100
admin> set atm-connect-options nailed-group = 101
admin> write -f
CONNECTION/sdsl1-t1000 written
```

Following is a comparable RADIUS profile:

```
permconn-st-1 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-CIR,
    User-Name = "sdsl1-t1000",
    Ascend-ATM-Group = 201,
    Ascend-Route-IP = Route-IP-No,
    Ascend-ATM-Vpi = 8,
    Ascend-ATM-Vci = 35,
    Ascend-ATM-Connect-Vpi = 1,
    Ascend-ATM-Connect-Vci = 100,
    Ascend-ATM-Connect-Group = 101
```

The following commands configure the first SDSL subscriber PVC:

```
admin> new connection term-sdsl1-1
CONNECTION/term-sdsl1-1 read
admin> set active = yes
admin> set encapsulation-protocol = atm
admin> set ip-options remote-address = 2.2.2.2/29
admin> set atm-options vpi = 0
admin> set atm-options vci = 100
admin> set atm-options nailed-group = 101
admin> set atm-options atm-circuit-profile = sdsl1-t1000
admin> write –f
CONNECTION/term-sdsl1-1 written
```

Following is a comparable RADIUS user profile:

```
permconn-st-1 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-1483,
```

```
    User-Name = "term-sdsl1-1",
    Framed-IP-Address = 2.2.2.2,
    Framed-IP-Netmask = 255.255.255.248,
    Ascend-ATM-Group = 101,
    Ascend-Route-IP = Route-IP-Yes,
    Ascend-ATM-Vpi = 0,
    Ascend-ATM-Vci = 100,
    Ascend-ATM-Circuit-Name = sdsl1-t1000
```

Defining the second PVC to be routed to the ISP

The following commands configure an ATM circuit between the second SDSL interface and the T1000 internal interface:

```
admin> new connection sdsl2-t1000
CONNECTION/sdsl2-t1000 read
admin> set active = yes
admin> set encapsulation-protocol = atm-circuit
admin> set ip-options ip-routing = no
admin> set atm-options vpi = 8
admin> set atm-options nailed-group = 202
admin> set atm-connect-options vpi = 1
admin> set atm-connect-options vci = 133
admin> set atm-connect-options nailed-group = 101
admin> write -f
CONNECTION/sdsl2-t1000 written
```

Following is a comparable RADIUS profile:

```
permconn-st-1 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-CIR,
    User-Name = "sdsl2-t1000",
    Ascend-ATM-Group = 202,
    Ascend-Route-IP = Route-IP-No,
    Ascend-ATM-Vpi = 8,
    Ascend-ATM-Vci = 35,
    Ascend-ATM-Connect-Vpi = 1,
    Ascend-ATM-Connect-Vci = 133,
    Ascend-ATM-Connect-Group = 101
```

The following commands configure the second SDSL subscriber PVC:

```
admin> new connection term-sdsl2-1
CONNECTION/term-sdsl2-1 read
admin> set active = yes
admin> set encapsulation-protocol = atm
admin> set ip-options remote-address = 3.3.3.3/29
admin> set atm-options vpi = 0
admin> set atm-options vci = 124
admin> set atm-options nailed-group = 101
```

```
admin> set atm-options atm-circuit-profile = sdsl2-t1000
admin> write –f
CONNECTION/term-sdsl2-1 written
```

Following is a comparable RADIUS user profile:

```
permconn-st-2 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-1483,
    User-Name = "term-sdsl2-1",
    Framed-IP-Address = 3.3.3.3,
    Framed-IP-Netmask = 255.255.255.248,
    Ascend-ATM-Group = 101,
    Ascend-Route-IP = Route-IP-Yes,
    Ascend-ATM-Vpi = 0,
    Ascend-ATM-Vci = 124,
    Ascend-ATM-Circuit-Name = sdsl2-t1000
```

Index

E

F

H

I

L

M

N

O

P

R

S

T

U

V

W