Lucent Technologies
Bell Labs Innovations

Stinger®

Administration Guide

Part Number: 7820-0712-006
For software version 9.5
August 2003

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. For latest information, refer to online product documentation at www.lucent.com/support.

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 easy 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 or release number
- Software and hardware options
- If supplied by your carrier, service profile identifiers (SPIDs) associated with your line
- 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 +1 510-747-2000 for an operator. You must have an active services agreement or contract.

Contents

Figures

Tables

About This Guide

This guide explains how to administer a Stinger unit and manage its operations. To use this guide, you must have set up the Stinger system as described in the *Getting Started Guide* for your Stinger unit and configured it for network connectivity as described in the *Stinger ATM Configuration Guide*.

What is in this guide

Each chapter in this guide focuses on a particular aspect of Stinger unit administration and operations. The chapters describe tools for system management, network management, and SNMP agent management.

To perform many of the tasks in this manual, you must have administrative permission on the Stinger unit. For instructions on logging into the Stinger unit with administrative permissions, see "Logging into a Stinger unit" on page 1-1.

Note This manual describes the set of features for Stinger units running software version TAOS 9.5-206.0. Some features might not be available with earlier versions or specialty loads of the software.

Warning Before installing or operating 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 your unit's *Getting Started Guide*s.

What you should know

This guide attempts to provide enough information to enable an administrator who is not an expert in a particular network technology to operate and troubleshoot a Stinger unit. However, this guide does not provide a complete explanation of any network management topic. For best results, when working with the following capabilities on a Stinger unit, make sure that you have some applicable general knowledge:

- Line configuration and testing
- Connection negotiation and authentication
- Connection cost management and accounting
- IP routing
- Network security

Documentation conventions

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

Convention	Meaning
`Monospace text`	Represents text that appears on your computer's screen, or that could appear on your computer's screen.
`Boldface monospace text`	Represents characters that you enter exactly as shown (unless the characters are also in ***`italics`***—see *Italics*, below). If you could enter the characters but are not specifically instructed to, they do not appear in boldface.
Italics	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[ ]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in boldface.
|	Separates command choices that are mutually exclusive.
>	Points to the next level in the path to a parameter or menu item. The item that follows the angle bracket is one of the options that appear when you select the item that precedes the angle bracket.
Key1+Key2	Represents a combination keystroke. To enter a combination keystroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl+H means hold down the Ctrl 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 Stinger platform. 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 on units that support it.
  - 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 integrate the Stinger into the ATM and Digital Subscriber Line (DSL) access infrastructure. The guide explains how to configure PVCs, and shows how to use standard ATM features such as quality of service (QoS), connection admission control (CAC), and subtending.
  - *Stinger IP2000 Configuration Guide*. For Stinger systems with the IP2000 control module, this guide describes how to integrate the system into the IP infrastructure. Topics include IP-routed switch-through ATM PVCs and RFC 1483 PVCs that terminate on the IP2000, IEEE 802.1Q VLAN, and forwarding multicast video transmissions on DSL interfaces.
  - *Stinger Private Network-to-Network Interface (PNNI) Supplement*. For the optional PNNI software, this guide provides quick-start instructions for configuring PNNI and soft PVCs (SPVCs), and describes the related profiles and commands.
  - *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.* For the optional T1000 module, this guide describes how to configure the Layer 3 routing and virtual private network (VPN) capabilities.
- **RADIUS:** *TAOS RADIUS Guide and Reference*. Describes how to set up a 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.

Administering a Stinger System 1

This chapter describes the system administration tasks that you might perform on the Stinger unit, such as enabling basic security, configuring system-wide settings, managing system configuration and flash cards, and managing user connections.

To use this chapter, you must have performed the tasks described in the *Getting Started Guide* for your unit and the *Stinger ATM Configuration Guide*. You can obtain the Stinger manuals at `http://www.lucentdocs.com/ins`.

Note On a Stinger MRT device, control module and line interface module (LIM) functions are incorporated into the unit's chassis. The terms *control module* and *LIM* in this guide refer to the control module and the LIM port functions on a Stinger MRT and not to physical modules.

Logging into a Stinger unit

When you log into a Stinger unit, you actually connect to its control module. If the Stinger unit contains two control modules, you can connect to either control module.

Note On units with redundant control modules, only one control module is active at a time. The secondary control module becomes the primary (active) control module if the primary control module can no longer support the Stinger unit. The unit transfers any configuration changes that you make on the primary control module to the

secondary control module, except for changes to IP addresses. Each control module must have a unique IP address.

To administer the system, you can log in from a PC connected to the control module's serial port, or from a workstation that has Telnet access to the system. When you log in, you are prompted for a username:

```
User:
```

To log in with administrative privileges, enter the default password (`Ascend`) assigned to the Stinger `admin` login at the factory:

```
User: admin
Password: Ascend
```

The name specified in the `name` parameter of the `admin user` profile appears as your system prompt. For example:

```
admin>
```

If you are already connected to the Stinger unit as a different user, use the `auth` command to log in as the administrator:

```
admin> auth user
Password:
```

For additional information about `user` profiles, see "Managing administrative access to the unit" on page 1-5.

Enabling basic security measures

The Stinger unit is shipped with certain default parameters set to allow easy access for the initial configuration. After you have initially logged in as administrator, ensure that the following three basic security tasks have been completed:

- Change the default `admin` password.
- Secure the serial port on both control modules.
- Specify one of the Ethernet ports as a management-only port.

You can also manage administrative access to the Stinger unit by specifying the types of tasks administrative users can perform on the Stinger unit. See "Managing administrative access to the unit" on page 1-5.

If the Stinger unit will be configured for SNMP, see also "Securing the SNMP agent" on page 9-4.

Changing the default Admin password

Because the `admin` login has superuser privileges, you must change the default password immediately. Be sure to write down the password you assign and store it in a safe place.

To change the password for the `admin` login, proceed as follows:

```
admin> read user admin
USER/admin read

admin> set password = top-secret

admin> write
USER/admin written
```

All subsequent administrator logins are required to supply the new password. (For more information about configuring `user` profiles, see "Managing administrative access to the unit" on page 1-5.)

Securing the serial port of each control module

The default settings for the control module allow anyone connecting to the serial port to access the system as the `admin` user, without logging in or being authenticated. Therefore, you must configure each control module to request a username and password and to automatically log the user out when the terminal session is terminated.

To secure the serial port on a single or primary control module, proceed as follows:

1 Read the `serial` profile of the primary (or single) control module:

```
admin> read serial {1 8 2}
```

The `serial` profile index refers to a physical port on the control module. The serial port is always designated as the second physical port of the control module.

2 Set the `user-profile` parameter to null:

```
admin> set user-profile =
```

3 Set the `auto-logout` parameter to `yes`:

```
admin> set auto-logout = yes
```

With this setting, the system automatically logs off the current `user` profile if the Data Terminal Ready (DTR) signal is lost on the serial port.

4 Write the profile:

```
admin> write
```

If your Stinger unit is operating with two control modules, both are working in parallel. As a result, the primary control module does not copy over this configuration to the secondary control module. You must secure both serial ports manually.

To secure the serial port on a secondary control module:

1 Read the `serial` profile of the secondary control module:

```
admin> read serial {1 9 2}
```

2 Set the `user-profile` parameter to null and the `auto-logout` parameter to `yes`:

```
admin> set user-profile =
admin> set auto-logout = yes
```

3 Write the profile:

```
admin> write
```

Now users connecting to a control module must supply a valid username and password for access to the Stinger unit.

Specifying a management-only Ethernet interface

You can specify that a control module's Ethernet interface is for management only. Following is the relevant parameter, which is shown with its default setting:

```
[in IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }]
management-only-interface = no
```

Setting the `management-only-interface` parameter to `yes` means that incoming traffic on the interface terminates in the system itself and is not forwarded on any other interface. In addition, only traffic generated by the system is forwarded onto the management-only interface. Traffic generated externally is dropped by the interface.

To configure a management interface for each of the control modules, proceed as in the following example:

```
admin> read ip-int {{ 1 8 1 } 0}
IP-INTERFACE/{ { shelf-1 slot-8 1 } 0 } read

admin> set management-only = yes

admin> write
IP-INTERFACE/{ { shelf-1 slot-8 1 } 0 } written

admin> read ip-int {{ 1 9 1 } 0}
IP-INTERFACE/{ { shelf-1 slot-9 1 } 0 } read

admin> set management-only = yes

admin> write
IP-INTERFACE/{ { shelf-1 slot-9 1 } 0 } written
```

Verifying the Ethernet port status

You can view the Ethernet's port status using the `ifmgr` command. For the system to respond to this command, your `user` profile must be enabled with debug privileges. For information on enabling debug privileges see "Enabling debug permissions" on page A-1.

To verify that an Ethernet interface has been set for management only, display the output of the `ifmgr -d` command, as shown in the following example:

```
admin> ifmgr -d
bif slot sif u m p ifname     host-name  remote-addr       local-addr
-------------------------------------------------------------------------
000 1:09 000 *     ie0        -          0.0.0.0/32        134.112.26.201/32
001 1:09 001 *     ie1        -          0.0.0.0/32        0.0.0.0/32
002 1:09 002 *     lo0        -          0.0.0.0/32        127.0.0.1/32
003 0:00 000 *     rj0        -          0.0.0.0/32        127.0.0.2/32
004 0:00 000 *     bh0        -          0.0.0.0/32        127.0.0.3/32
005 1:09 000 *     wanabe     -          0.0.0.0/32        127.0.0.3/32
006 0:00 000 *     local      -          0.0.0.0/32        127.0.0.1/32
007 0:00 000 *     mcast      -          0.0.0.0/32        224.0.0.0/32
008 0:00 000 -     tunnel0    -          0.0.0.0/32        134.112.26.201/32
009 0:00 000 *     vr0_main   -          0.0.0.0/32        134.112.26.201/32
010 0:00 000 -     sip0       -          0.0.0.0/32        0.0.0.0/32
011 1:05 006 *   p wan11      bir-2-2    222.222.222.222/32 222.222.222.1/32
```

The `u` column displays an asterisk (*) to indicate that the interface is operational or a hyphen (-) to indicate that it is disabled.

Managing administrative access to the unit

You create and define administrative access to the Stinger unit using `user` profiles. Do not confuse them with `connection` profiles. You configure `user` profiles to provide access to the Stinger command-line interface to monitor or configure the unit. In contrast, `connection` profiles contain authentication and configuration information for a remote device or user and allow the remote user to connect to the Stinger unit for WAN or LAN access.

You can create any number of `user` profiles and fine-tune the privileges they allow. In addition to authentication and permission information, `user` profiles also contain parameters that affect how the user's environment appears at login.

A Stinger unit is shipped with the predefined `user` profiles `admin` and `default`. An `admin user` profile provides full read-write permissions, while the `default user` profile authorizes minimal use of commands.

Many sites choose to create some administrative accounts with read-only permissions, to allow certain users to check status windows, read log buffers, and enter diagnostic commands. You need at least one administrative account with read-write permissions, but you might choose to create several read-only accounts.

For information about managing administrative sessions, see "Managing administrative connections" on page 1-45.

Logging into the Stinger unit

To log into the Stinger unit for administrative tasks, use a profile that has write permissions, as in the following example:

```
% telnet myStinger
User: admin
Password: mypassword

admin>
```

If you are already logged into the Stinger unit, make sure you are at the highest level by entering the `list ..` command (possibly more than once), as in the following example:

```
admin> list ..
name = ""
physical-address* = { shelf-1 slot-1 1 }
line-interface = { yes esf b8zs eligible middle-priority inband wink-start
digi+

admin> list ..
error: at highest level
```

Creating a new user profile

To create a new `user` profile based on the `user` profile `admin`, append `admin` to the `new user` command. The following example shows how to create a new `user` profile named `test`, with full administrative privileges:

```
admin> new user admin
USER/admin read

admin> set name = test
```

```
admin> set password = test-pw
admin> write
USER/admin written
```

To create a new `user` profile based on the `user` profile `default`, use the `new user` command with no additional arguments. The following example shows how to create a new user profile named `test2`, with default administrative privileges:

```
admin> new user
USER/default read
admin> set name = test2
admin> set password = my-password
admin> write
USER/test2 written
```

Activating and authenticating a `user` profile

To activate a `user` profile, proceed as follows:

```
admin> read user test
USER/test read
admin> set active-enabled = yes
admin> write
USER/test2 written
```

If you are connected to the Stinger unit as a different user, use the `auth` command to log in as the administrator:

```
admin> auth user
Password:
```

Assigning permissions

If you have administrative privileges, you can create any number of `user` profiles that grant other administrators various degrees of access to the system.

You can set the following permission parameters in any combination:

Parameter	Setting
`allow-code`	Enable/disable permission to upload code to the Stinger unit and use the following code-level commands: ■ `format`—Prepares a flash card for use ■ `fsck`—Checks the file system on a flash card
`allow-diagnostic`	Enable/disable administrative access to diagnostic profiles.
`allow-password`	Enable/disable administrative access to the password command.
`allow-system`	Enable/disable administrative access to system profiles.
`allow-termserv`	*Does not apply to the Stinger unit.* Enable/disable administrative access to the terminal-server commands.
`allow-update`	Enable/disable administrative access to update profiles.

Parameter	Setting
`allow-debug`	Enable/disable administrative access to debug commands. This parameter is not visible on the interface. See "Enabling debug permissions" on page A-1.

Understanding command permissions

Permissions control the actions that a user who logs in with a particular profile can perform on a Stinger unit. Each permission enables the use of a particular command *class*. When you use the `help` command to display available commands, the left column shows command names, and the right column shows the command class. For example:

```
admin> ?
?                              ( user )
 acct-failsafe                  ( debug )
 agsh                           ( debug )
 alarm                          ( system )
 aliasTable                     ( debug )
 annexType                      ( debug )
 apsMgr                         ( debug )
 arptable                       ( system )
 atmcacstat                     ( debug )
 atmCacToggle                   ( debug )
 atmCktState                    ( debug )
 atmConnectionFailures          ( system )
 atmControlState                ( debug )
 atmDelGet                      ( debug )
 atmds3trunkdev                 ( debug )
 atme3trunkdev                  ( debug )
 atmems                         ( debug )
 AtmEmsDebug                    ( debug )
 atmFlexVpiVci                  ( debug )
 atmGet                         ( debug )
 atmInternalLines               ( system )
 atmnbase                       ( debug )
[More? <ret>=next entry, <sp>=next page, <^C>=abort]
```

Typically, read-write accounts enable the System command class. They might also enable the Update and Code command classes. Read-only accounts might be limited

to the Diagnostic command class. Table 1-1 shows the commands associated with each permission.

Table 1-1. Permissions and associated commands

Permission	Command class	Commands in this class	
N/A (always enabled)	User	?	grep
		auth	help
		clear	prtcache
		date	quit
		dtunnal	sleep
		filtcachgre	whoami
		gre	who
Allow-System	System	alarm	new
		arptable	ospf
		atminternallines	ospfd
		atmqos	pnnidisplay
		atmsig	pnniinterfacedisplay
		atmtrunks	pnnilinkdisplay
		atmvccstat	pnnimapdisplay
		atmvcl	pnninbrdisplay
		atmvpl	pnninodedisplay
		atmvcx	pnninodetopology
		atmvpx	pnniptsestatus
		brichannels	pnnireachableaddr
		clr-history	pnniroutebase
		cltactivate	read
		cltcmd	rearslotshow
		cltdeactivate	redprofsync
		connection	redundant-controller-
		dir	switch
		dircode	refresh
		dmtaldsllines	screen
		dsllines	sdsllines
		fatal-history	shdsllines
		get	set
		hdsl2lines	show
		imagroups	spvcc
		imalines	spvcshow
		ipcache	spvcstat
		ipportmap	spvpc
		iproute	status
		isolate	userstat
		line	version
		list	view
		log	which
		netstat	

Table 1-1. Permissions and associated commands (Continued)

Permission	Command class	Commands in this class	
Allow-Update	Update	delete load nvram reset	save snmpauthpas snmpprivpass write
Allow-Code	Code	format	fsck
Allow-Diagnostic	Diagnostic	atmtrunkmgr atmtrunkreset clock-source debug device ether-display if-admin ledoff nslookup oam oamloop open ping relayoff	remote slot slot-clock-source telnet traceroute tramtprx trapdump uds3dump uptime wandisplay wandess wannext wanopening
Allow-Termserv	Termserv	terminal-server *Does not apply to the Stinger unit.*	
Allow-Password	N/A	The Allow-Password permission enables the user to view passwords. If the permission is set to no, the user sees a row of asterisks instead of the actual configured password. If the administrator who backs up system configurations does not have the allow-password permission set to yes, passwords are not saved as part of the configuration.	

Typical permission configurations

The following commands create a read-write administrative login named Marco, which is based on the admin user profile, but has access only to System, Diagnostic, and Update command classes:

```
admin> new user admin
USER/admin read

admin> set name = marco

admin> set password = my-password

admin> set allow-password = yes

admin> set allow-code = no

admin> write
USER/marco written
```

The following commands create a `user` profile named `test` based on the `user` profile `admin`, but restricts some permissions and assigns a different password:

```
admin> new user admin
USER/admin read
admin> set name = test
admin> set password = test-pw
admin> set allow-update = no
admin> set allow-code = no
admin> write
USER/admin written
```

The following commands create a profile that enables the user to use the update commands, but not to perform any other actions:

```
admin> new user
USER/default read
admin> set name = techpubs
admin> set password  = january
admin> set allow-update= yes
admin> set prompt = *
admin> set log-display-level = none
admin> write
USER/techpubs written
```

Specifying group permissions

You can create a centralized definition of the TAOS commands that a group of users can perform, and associate individual users with a command user group. You use the `user-group` profile to define command access for a group of users you specify. Then, you assign a user group to a user by specifying a valid `user-group` profile for the `user-group` parameter in the `user` profile.

Creating a user group

To define a command user group, specify the following parameters in the `user-group` profile. You can specify access settings and a list of up to 512 commands that users in the command user group have permission to use.

Parameter	Setting
`name`	Name of a command user group. Specify up to 23 characters. The default is null.

Parameter	Setting
use-group-permissions	Enable/disable the user's access to all the allow-*xxx* settings in the user-group profile specified by the user-group parameter. With the default no setting, the user does not have access to the commands permitted by the allow-*xxx* settings in the user-group profile and only the commands permitted by the allow-*xxx* settings in the user profile apply. Specify yes for the user to have access to all commands permitted by the allow-*xxx* setting in the user-group profile and for the allow-*xxx* settings in the user profile to be ignored.
allow-termserv	Enable/disable permission for the users in the group to use terminal-server commands. With the default no setting, users do not have terminal-server permission. Specify yes to enable users to have terminal-server permission.
allow-system	Enable/disable permission for the users in the group to use system-level commands. With the default no setting, users do not have system-level permission. Specify yes to give users system-level permission.
allow-diagnostic	Enable/disable permission for the users in the group to use diagnostic-level commands. With the default no setting, users do not have diagnostic-level permission. Specify yes to give users diagnostic-level permission.
allow-update	Enable/disable permission for the users in the group to use update-level commands. With the default no setting, users do not have update-level permission. Specify yes to give users update-level permission.
allow-password	Enable/disable permission for the users in the group to view passwords. With the default no setting, users cannot view passwords. Specify yes to enable users to view passwords.
allow-code	Enable/disable permission for the users in the group to use code-level commands. With the default no setting, users do not have code-level permission. Specify yes to give users code-level permission.
exclude-listed-commands	Enable/disable permission for the users in the group to use the commands designated by the command parameter. With the default no setting, users have permission to use the designated commands. Specify yes to disable permission to use the designated commands.
command [*n*]	Commands to allow or exclude.

Specifying a command user group for a user

You assign a command user group to a user by specifying a valid `user-group` profile name for the `user-group` parameter in the `user` profile. Following is the definition for the `user-group` parameter:

Parameter	Setting
`user-group`	Name of a `user-group` profile. The default is null. If the `user-group` parameter refers to a valid `user-group` profile, the access settings of the `user-group` profile are applied to the user session, overriding those in the `user` profile. If the `user-group` profile cannot be found, the user cannot log on or perform any commands. If no `user-group` profile is specified in the `user` profile, the access settings in the `user` profile apply.

Sample command user group configuration

In this example, the existing user `bill` is given permission to use the six commands that he needs to provision new users. The existing user `ted` can use all the Stinger commands except `reset`, `slot`, and `read`:

```
admin> read user bill
USER/bill read
admin> set user-group = provisioning
admin> write -f
USER/bill written
admin> new user-group provisioning
USER-GROUP/provisioning read
admin> set command 1 = new
admin> set command 2 = list
admin> set command 3 = delete
admin> set command 4 = write
admin> set command 5 = get
admin> set command 6 = auth
admin> write -f
USER-GROUP/provisioning written
admin> read user ted
USER/ted read
admin> set allow-update = yes
admin> set allow-system = yes
admin> set allow-termserv = yes
admin> set allow-diagnostic = yes
admin> set allow-password = yes
admin> set allow-code = yes
admin> set user-group = maintenance
```

```
admin> write -f
USER/ted read

admin> new user-group maintenance
USER-GROUP/maintenance read

admin> set use-group-permissions = yes

admin> set exclude-listed-commands = yes

admin> set command 1 = reset

admin> set command 2 = slot

admin> set command 3 = read

admin> write -f
USER-GROUP/maintenance written
```

When you change the `user-group` settings, the permissions of the associated users are automatically adjusted. If a `user-group` profile is deleted, the sessions of all the associated users are terminated.

Verifying user group settings

The system does not prohibit you from entering a command user group or a user that does not exist, nor from entering an invalid list of commands. Use the `usergroupcheck` command to verify that your specifications are valid. For syntax information, see the *Stinger Reference*.

To verify that all the `user-group` profiles specify valid lists of commands and that all `user-group` profiles specified by `user` profiles are valid, use the `usergroupcheck` command with the `-a` option. For example:

```
admin> usergroupcheck -a
All groups and users verified
```

To verify that the `user-group` profile specified in the `user` profile enter the `usergroupcheck` command with the `-u` option. For example:

```
admin> usergroupcheck -u bill
Group provisioning: Commands all valid.
Commands available to this user are:
     ?                              ( user )
     auth                           ( user )
     clear                          ( user )
     date                           ( user )
     delete                         ( update )
     dtunnel                        ( user )
     filtcache                      ( user )
     get                            ( system )
     gre                            ( user )
     grep                           ( user )
     help                           ( user )
     l2tp                           ( user )
     l2tpcards                      ( user )
     l2tpsessions                   ( user )
     l2tptunnels                    ( user )
     list                           ( system )
     netware                        ( user )
```

```
new                             ( system )
prtcache                        ( user )
quit                            ( user )
whoami                          ( user )
write                           ( update )
```

To verify the `user-group` profile specified by the `user-group` parameter in the `user` profile called *`user`*, and display the commands to which *`user`* has access, use the `-g` *`group`* option. For example, the following example verifies that the `newyork` command user group contains a valid list of commands:

```
admin> usergroupcheck -g newyork
Group provisioning commands all valid
```

Extra levels of security

Certain command options have extra levels of security restricting access beyond that of standard commands, and these security levels cannot be bypassed by means of the `user-group` profile. For example, the standard `arptable` command displays the contents of the ARP cache, and is protected by the `system` level in both the `user` and `user-group` profiles. In addition, the option to add entries to the table is protected by the `diagnostic` or `update` level. As a result, allowing a command user group access to the `arptable` command by designating it with the `command` parameter does not allow members of the group to add entries to the ARP cache, unless the group or any of its users is granted access to system, diagnostic, and update commands.

Following are other commands and options that have additional levels of security:

- `arptable -a`—Protected by update or diagnostic permission.
- `arptable -d`—Protected by update or diagnostic permission.
- `arptable -f`—Protected by update or diagnostic permission.
- `loadmate`—Protected by debug and code permissions.
- `filtcache -f`—Protected by update or diagnostic permission.
- `prtcache -f`—Protected by update or diagnostic permission.
- `resrcmgr -t`—Protected by diagnostic permission.

When used to restore configurations, the `load` command also requires the use of the `new`, `set`, and `write` commands, because the device runs these commands in the process of loading the configuration.

Specifying a time-out for user logins

You can specify a time-out period after which idle sessions on the Stinger unit disconnect. The default is 60 seconds. To configure an idle time-out, proceed as in the following example:

1 Read the `user` profile.

```
admin> read user test
```

2 Specify an idle time period.

```
admin> set idle-logout = 120
```

3 Write the profile.

```
admin> write
User test written
```

Setting the command-line prompt

The command-line prompt is configured with the `prompt` parameter. To configure a command-line prompt of `hello` to be displayed for the user `test`, proceed as follows:

1 Read the `user` profile.

```
admin> read user test
```

2 Specify the prompt.

```
admin> set prompt = hello
```

3 Write the profile.

```
admin> write
User test written
```

The default command-line prompt is an asterisk followed by a right angle bracket (`*>`). An asterisk in this setting causes the Stinger system to substitute the value of the profile's `name` parameter after a successful login. For example, for the `admin` profile, the following prompt appears:

```
admin>
```

Setting log levels for each login

You can configure the `user` profile to display one or more levels of log messages immediately in the interface. The display level you set causes messages at that level and above to be displayed in the interface, interrupting whatever work might be going on at the prompt. For example, the following commands cause messages at the critical, alert, and emergency levels to be displayed:

```
admin> read user test
USER/test read

admin> set log-display-level = critical

admin> write
USER/test written
```

Table 1-2 lists the message levels in order from highest to lowest severity.

Table 1-2. Message level severity

Message level	Indicates
`emergency`	Error condition in the Stinger unit. The unit is probably not operating normally.
`alert`	Error condition in the unit. However, the unit is still operating normally.
`critical`	Inoperative interface or a security error.
`error`	Error event.
`warning`	Unusual event (a user entering an incorrect password, for example). However, the unit is otherwise operating normally.

Table 1-2. Message level severity

Message level	Indicates
notice	Event of interest in normal operation (for example, the establishment of a link).
info	State or status change that is not of general interest.
debug	Helpful debug information.
none	No messages are displayed.

Logging in as a different user

To log in with a different user profile, use the auth command, as in the following example:

```
admin> auth test
Password:@3wPZHd2
```

You must supply the password configured in the specified profile to be logged in as the user. Logging in as a different user can be helpful for verifying that the user profile permissions are correct.

Displaying the current user

To display the user profile that you are currently using, enter the whoami or who am i command. For example:

```
admin> whoami
User Name : admin User Profile : admin
```

Working with the system profile

The system profile contains system-wide configuration settings. Most of these parameters are set during initial configuration.

Following is a listing of system profile parameters. For additional parameter information, see the *Stinger Reference*.

```
[in SYSTEM]
name = ""
system-rmt-mgmt = yes
use-trunk-groups = no
num-digits-trunk-groups = 1
idle-logout = 0
max-dialout-time = 20
parallel-dialing = 12
single-file-incoming = yes
exclusive-port-routing = no
high-ber-alarm-threshold = 10-**-3
high-ber-alarm = no
no-trunk-alarm = no
```

```
sessionid-base = 0
call-routing-sort-method = item-first
digital-call-routing-sort-method = slot-first
exact-match-call-routing = no
shelf-controller-type = standalone
master-shelf-controller = 1
new-nas-port-id-format = yes
perm-conn-upd-mode = all
userstat-format = "%i %l %s %r %d %a %u %c %t %n"
control-bus-type = dpram
boot-cm-version = 9.5-206.0
system-8k-clock = controller
ignore-lineup = no
nvram-was-rebuilt = no
connection-profile-auto-naming-convention = lower-interface-number-first
link-phys-trap-state = trap-state-enabled
link-perm-trap-state = trap-state-enabled
```

Setting the system name

The Stinger system name is used only during Point-to-Point Protocol (PPP) negotiations. The name is not used in Domain Name System (DNS) lookups.

The system name is specified in the `system` profile. For example, to set the Stinger unit's system name to `Stinger01`, proceed as follows:

```
admin> read system
SYSTEM read

admin> set name = Stinger01

admin> write
SYSTEM written
```

Configuring system clocking

The Stinger unit requires a clock source for its timing subsystem. By default, the system uses the a built-in 8kHz clock on the single or primary control module as its timing source. The `system-8k-clock` parameter in the `system` profile specifies the clock source for the Stinger system. You can configure the system to take its clock source from a line interface module (LIM), trunk port, or from an external building integrated timing supply (BITS) clock connected to the unit's alarm relay. By default, the `system-8k-clock` parameter is set to `controller`.

Displaying the current clock-source

You can view the current clock source by using the `get` command to display the setting for the `system-8k-clock` parameter. For example:

```
admin> get system system-8k-clock
[in SYSTEM:system-8k-clock]
system-8k-clock = controller
```

The `clock-source` command also displays the current clock-source along with available clock sources.

```
admin> clock-source
Master: slot-1/1 line 3
Source List:
    Source: slot-1/1 Available      priority: 1
```

A line specified as the clock source can be used as the source of timing information for synchronous connections, so both the sending device and the receiving device can determine where one block of data ends and the next begins. If multiple lines specify that they are the clock-source (the default configuration), you can assign clock-source priority among multiple lines.

The following commands cause the system to first attempt to use a trunk port as its clock source, and to use the built-in clock only if it finds no ports that are eligible clock sources:

```
admin> read system
SYSTEM read
admin> set system-8k-clock = lim-or-trunk-module
admin> write
SYSTEM written
```

Configuring trunk ports as clock sources

You can specify whether a trunk port can be used to source the ATM network clock and feed it to the primary control module as the master clock for the unit. To specify whether a trunk port as eligible or ineligible for this use, set the `clock-source` parameter in the trunk profile for that port (`ds3-atm`, `oc3-atm`, or `e3-atm` profile). You can assign a high, middle, or low priority for being elected as the clock source by setting the `clock-priority` parameter in the trunk profile for that port.

If more than one line is eligible to be the clock source, the system chooses the one with the highest priority, as specified by the `clock-priority` setting. If multiple sources of equal priority are present, the system selects the first valid clock source. (A clock source is valid if the `clock-source` parameter is set to `eligible` and the OC12, DS3, OC3, or E3 interface is synchronized.)

Once it has selected a clock source, the system uses that source until the source becomes unavailable or a higher-priority source becomes available. If no eligible external sources exist, the system uses an internal clock generated by the primary control module.

The following sample commands configure both ports of the first DS3-ATM module as eligible clock sources, with the first port assigned a higher priority for this use:

```
admin> read ds3-atm { 1 trunk-module-1 1 }
DS3-ATM/{ shelf-1 trunk-module-1 1 } read
admin> set line-config clock-source = eligible
admin> set line-config clock-priority = high
admin> write
DS3-ATM/{ shelf-1 trunk-module-1 1 } written
admin> read ds3-atm { 1 trunk-module-1 2 }
DS3-ATM/{ shelf-1 trunk-module-1 2 } read
admin> set line-config clock-source = eligible
admin> set line-config clock-priority = low
```

```
admin> write
DS3-ATM/{ shelf-1 trunk-module-1 2 } written
```

The following commands configure only the first port of the second OC3-ATM trunk module as an eligible clock source. If this port becomes unavailable and is not backed up, the unit begins using the built-in clock on the primary control module.

```
admin> read oc3-atm { 1 trunk-module-1 1 }
OC3-ATM/{ shelf-1 trunk-module-1 1 } read

admin> set line-config clock-source = eligible

admin> set line-config clock-priority = high

admin> write
OC3-ATM/{ shelf-1 trunk-module-1 1 } written
```

The *Getting Started Guide* for your unit provides additional information about configuring the system clock source.

Setting the system time and date

The Stinger unit maintains the time and date. For proper operation, set the time and date at initial configuration using the `timedate` profile.

Viewing the system time and date

To view the current time and date, enter the `date` command with no argument. For example:

```
admin> date
Tue Nov  6 14:52:25 2001
```

You can also access the `timedate` profile to view the information:

```
admin> get timedate
[in TIMEDATE]
time = { 14 53 10 }
date = { Tuesday November 2001 6 }
```

Changing the system time

If the time is incorrect, you can change it by entering the current time in the `timedate` profile. The following example shows how to change the system time to 12:30:08 a.m.:

```
admin> read timedate
TIMEDATE read

admin> set time = { 12 30 08 }

admin> write
TIMEDATE written
```

Changing the system date

If the date is incorrect, you can change it by entering the current time in the `timedate` profile. Because the `date` subprofile includes a read-only field (day of week), you must set the date parameters independently. The following example shows how to change the system date to January 6, 2002.

```
admin> read timedate
TIMEDATE read
admin> set date month = 01
admin> set date day = 06
admin> set date year = 2002
admin> write
TIMEDATE written
```

Managing system configuration

The system's configuration is stored in the onboard nonvolatile random access memory (NVRAM). The configuration can be saved, restored, or cleared as needed.

The `nvram` command provides functions for managing and clearing onboard memory. For syntax information, see the *Stinger Reference*.

Caution Make sure you have a recent backup before using the `nvram` command. (See "Saving the configuration" on page 1-20.)

Displaying NVRAM usage statistics

To display NVRAM usage information, specify the `-u` option:

```
admin> nvram -u
Not Using Extended profiles
NVRAM seg[0]:start 80bb9728 size 262136 avail 199480 used 62656 cmpct 0
NVRAM seg[1]:start 80bf9728 size 262136 avail 262136 used 0 cmpct 1
NVRAM seg[2]:start 80c39728 size 262136 avail 262136 used 0 cmpct 1
```

Clearing the configuration

To clear NVRAM, restoring the single or primary control module to its initial, unconfigured state, enter the NVRAM command without specifying an option:

```
admin> nvram
Clear configuration and reboot? [y/n]
```

To clear NVRAM and enter debug mode, use the `-t` option:

```
admin> nvram -t
```

To clear NVRAM and reset both control modules with no confirmation, proceed as follows:

```
admin> nvram -f -r both_controllers
Please standby. System reset in progress.
```

Note You must reset the Stinger unit after clearing NVRAM.

Saving the configuration

The `save` command saves all configured profiles, all profiles of a specified type, a specific profile to a file on a local disk or to a file on a network host. You can then use that file to restore the Stinger unit's configuration. To maintain redundancy

functionality, red copy the configuration on the primary control module to the configuration on the secondary control module. For syntax information, see the *Stinger Reference*.

Note To save passwords, you must have sufficient permissions to view password fields. (For a discussion of permissions, see "Understanding command permissions" on page 1-7.) Without this permission, passwords are not properly saved.

Saving the configuration to a local file

To save the Stinger configuration to a file on the system you are using to access the Stinger unit, enable the capture function in your VT100 emulation software, and enter the `save` command as follows:

```
admin> save -a console
```

The `-a` option saves all parameters, even those that are set to their default values. You might want to print a copy of the configuration for later reference.

The entire configuration is written to the specified file. This method allows you to cut and paste the configuration to other devices.

Saving the configuration to a network host

To save the configuration on a network host, you must specify the hostname and the full path of a filename. In the following example, `host1` is the network host and `saved.cfg` is the filename:

```
admin> save -a network host1 saved.cfg
configuration being saved to host 10.65.212.19 file saved.cfg...
connection saved.
```

Saving the configuration in GZIP compressed format

You can save the configuration file of a Stinger unit in gzip compressed format. The GZIP compressed format enables you to reduce the size of the configuration file, reduce the time required to save the file over a low bandwidth administrative link, improve performance when Stinger management is done using configuration file exchange with NAVIS™ management software.

If you use the `-z` option with the `save` command, configuration output is compressed before being sent to a network storage location via TFTP. If you use the `-z` option with the `-e` option, the configuration output is compressed first and then encrypted.

The following sample command saves all fields, even those with default parameters, to a gzip compressed file on a network host at `192.168.1.1`, under the file name `saved.cfg`.

```
admin> save -a -z network 192.168.1.1 saved.cfg
```

The `load` command automatically processes configuration files that have been saved in the gzip compressed format.

Compressing and uncompressing files on a flash card

To compress an existing file on a flash card, use the `gzip` command. To uncompress a file on the flash card that have been compressed by the `gzip` command, use the

gunzip command. The system-level gzip and gunzip commands function just like the UNIX gzip and gunzip commands. For syntax information, see the *Stinger Reference*.

Note Due to differences in implementation, files compressed with the TAOS gzip command may not be identical to files compressed with the UNIX gzip command. However, the compressed output files are completely compatible.

The following example compresses and replaces a file named save.conf in the zz subdirectory of flash card number 1 at the best level of compression. The resulting file is named save.conf.gz.

```
admin> gzip -9 1/zz/save.conf
```

The following sample command uncompresses and replaces a file named save.conf.gz in the zz subdirectory of flash card number 1. The resulting uncompressed file is saved as save.conf.

```
admin> gunzip 1/zz/save.conf.gz
```

To view file sizes after compressing and uncompressing files, use the ls command. for example:

```
admin> ls
ls Flash card 1:
/:
  current/                    0 Mon Jun  9 16:40:50 2003
  z/                          0 Mon Jun  9 16:42:18 2003
/current:
  stngrcm.ffs           4477734 Tue Jul  1 10:00:24 2003 Version 9.5-206.0e0
  stngrrsdsl.ffs        1013721 Tue Jul  1 10:00:40 2003 Version 9.5-206.0e0
  stngrt1000.ffs        1314833 Tue Jul  1 10:01:02 2003 Version 9.5-206.0e0
/z:
  save.conf              1439600 Fri Jun 27 16:45:56 2003

Total space:   31997952 bytes
       used:    8347648 bytes
       free:   23650304 bytes
```

Restoring or updating the configuration

You can restore a full configuration that you saved with the save command by means of the load command. The load command uploads a code image to flash or runs a remote configuration script. The code image or script can be located on the disk of the PC you are using for the terminal session with the Stinger unit, on a network host that supports TFTP, or on the PCMCIA flash card file system of the control module.

For syntax information, see the *Stinger Reference*.

Note You must reset the Stinger unit after reloading a configuration.

Restoring from a local file

Before you start the restore procedure, verify that your terminal emulation program has an autotype (or ASCII file upload) feature. Autotype allows your emulator to transmit a text file over its serial port. You must also verify that the data rate of your terminal emulation program is set to 9600 baud or lower and that the term-rate

parameter in the `system` profile is set to the same rate. Speeds higher than 9600 baud might cause transmission errors.

To restore a configuration from a file on the system you are using to access the Stinger unit, set your VT100 emulation software to send the file, and enter the `load` command as follows:

```
admin> load config console
```

Restoring from a network host

To restore a configuration from a file on a network host, enter the `load` command as follows:

```
admin> load config network hostname filename
```

Replace `hostname` with the name of the host and `filename` with the name of the file in which the configuration is stored.

For example, to load a configuration file named `unit.cfg` from network host 10.8.7.2 to the PCMCIA flash card in slot 1, proceed as follows:

```
admin> load config network 10.8.7.2 /unit.cfg
```

To load the `unitrel.tar` file from a network host named `host1`, proceed as follows:

```
admin> load tar network host1 unitrel.tar
```

Updating the configuration

You can use the `load` command to upload code for any module to a PCMCIA flash card. For example, to load the Stinger control module image `stngrtcm.ffs` from a TFTP server `pclab-20` to the secondary control module, proceed as follows:

```
admin> load -t cm network pclab-20 stngrtcm.ffs
loading code from 207.137.197.90
file stngrtcm.ffs...
done.
Attempting to write image(s) to other controller
Trying device 1 of remote controller first
Transferring 1/current/stngrtcm.ffs ...
done.
1 image successfully transferred
```

To load the Stinger tar image `stngrrel.tar` from TFTP server `pclab-20` and copy all images to the secondary control module, proceed as follows:

```
admin> load -t tar network pclab-20 stngrrel.tar
loading code from 207.137.197.90
file stngrrel.tar...
untaring and loading image for...
cm (stngrcm/stngrcm.ffs)...
sdsl-atm-card (stngrcsdsl/stngrcsdsl.ffs)...
al-dmtadsl-atm-card (stngrcaldsl/stngrcaldsl.ffs)...
done.
Attempting to write image(s) to other controller
Trying device 1 of remote controller first
Attempting to transfer all loads
Transferring 1/current/stngrcm.ffs ...
done.
```

```
Transferring 1/current/stngrcsdsl.ffs ...
done.
Transferring 1/current/stngrcaldsl.ffs ...
done.
3 images successfully transferred
```

Note You can set parameters in the `load-select` profile to specify which control module images to load to flash when you use a `load tar` command. However, an explicit `load` command for a particular module type overrides the settings in the `load-select` profile.

Transferring code images between control modules

On a Stinger FS, Stinger FS+, Stinger LS, or Stinger RT unit with dual control modules, you can transfer code images from one control module to the other using the `loadmate` command. Both control modules must be running TAOS 7.11.2 or later releases.

The `loadmate` command can perform the following operations:

- Transfer all images from one control module's PCMCIA flash card to the other control module's flash card.
- Transfer a specific code image, such as a load for a particular module, from one control module to another.
- Transfer a specific boot image from one control module to another.
- Transfer generic files. If the directory structure does not exist on the other control module, it is created.

The `loadmate` command supports all load types supported by the `load` command, with the exception of `config` and `tar`. You can use the command from either the primary control module or the secondary control module, in both boot or operational images. Images are copied from the control module from which the command is issued.

For the syntax of the `loadmate` command, see the *Stinger Reference*.

For example, to copy the control module's image from PCMCIA flash card 1 of the control module in slot 8 to flash card 1 of the control module in slot 9, enter the following command on the control module in slot 8:

```
admin> loadmate cm 1 1
```

To copy boot image 2 on the control module in slot 8 to the onboard flash memory of the control module in slot 9, enter the following command on the control module in slot 8:

```
admin> loadmate boot
```

To transfer all images of any known load type on flash card 1 of the control module in slot 9 to flash card 2 of the control module in slot 8, enter the following command on the control module in slot 9:

```
admin> loadmate 1 2 (executed )
```

You cannot run a `load` and `loadmate` operation or two `loadmate` operations simultaneously. Troubleshooting the restore process

If the system terminates the process of loading a tar file, one of the following messages might appear:

```
load aborted: not a tar image
load aborted: a tar image, inconsistent with the specified load-type.
load aborted: invalid/unknown image header.
load aborted: mismatched image for the specified load-type.
load aborted: invalid image, unsupported by load tar command.
```

The `load` command supports type checking to verify that the load type specified on the command line matches the image header. The preceding messages indicate that the type checking process discovered inconsistencies between the load type and the image header. Check your command line and, if necessary, download the tar file again.

The following warning message does not terminate the load operation, but indicates that you are not loading the most recent software version:

```
load: warning: old image header version detected, load continued...
```

Finally, the following error messages can also appear when you use the `load` command to upload an image to a PCMCIA flash card on a Stinger unit:

Message	Explanation
`load: error: flash card write failed: card full`	The flash card currently has no space available to load software.
`load: error: specified flash card not present`	No flash card is detected in the specified slot (1 or 2).
`load: error: specified flash card not formatted`	You must use the `format` command to format the flash card before loading the software.
`load: error: specified flash card has obsolete format`	You must use the `format` command to format the flash card, because a 1.3A file system was detected.
`load: error: specified flash card is write-protected`	The flash card's write-protect switch is set.
`load: error: specified flash image is currently in use`	A controller module in the LOAD state is currently accessing the flash card.

Using FTP to transfer files

You can use the File Transfer Protocol (FTP) client to transfer files larger than the TFTP limit of 16MB and to provide a more reliable file transfer protocol. You can start up the FTP client by entering the `ftp` command along with command line options. Alternatively, you can specify an FTP URL in the command line to initiate FTP.

To use the FTP client capability, your unit must have a file allocation table (FAT)-formatted flash memory card in its PCMCIA slot.

The FTP client supports active connections only. In addition, you cannot cancel an FTP download or upload that is already in progress.

FTP client command-line interface

The command interface to the TAOS FTP client consists of a subset of the FTP service commands defined in RFC 959, *File Transfer Protocol (FTP)*. You use these commands

to set the FTP file transfer type and working directory, to transfer files, and to otherwise manipulate FTP as you require.

To launch the FTP client, enter the `ftp` command at the command line prompt. The command has the following syntax:

`ftp` [***`options`***] [***`hostname`***] [***`port`***]

In this TAOS version, you can replace `options` with the following:

`-s` ***`Source IP Address`***

Replace `hostname` with the name of an FTP server. You can specify a value for `port` if the FTP server is running on a nondefault FTP port. The default port is 21.

If you provide a hostname, the FTP client attempts to connect and log in to the remote host. If you do not provide a hostname, the system displays the following prompt:

```
ftp>
```

At this prompt, you can enter the FTP service command `open` to connect to a particular FTP host. For a description of `open` and the other FTP service commands, see the *Stinger Reference*.

Typical command-line FTP file transfer

The following example shows a File Transfer Protocol connecting to a FTP server, logging in with a name and password, changing the current working directory on the server, changing the local current working directory, switching to binary transfer mode, downloading a binary file, and quitting the application.

```
admin> ftp 111.11.26.12
220 ds2 FTP server (SunOS 5.6) ready.
Name:ddoug
331 Password required for ddoug.
Password:
230 User ddoug logged in.

ftp> cd /tftpboot/ddoug
250 CWD command successful.

ftp> lcd current
Local directory now 1/current

ftp> binary
200 Type set to I.

ftp> get stngrcm.ffs
200 PORT command successful.
150 Binary data connection for stngrcm.ffs
(149.52.26.125,7018) (2258239 bytes).
2258239 bytes recieved in 30 seconds
226 Binary Transfer complete.

ftp> quit
221 Goodbye.
```

The following command shows how to connect to an FTP server and specify a source IP address of 1.1.1.1:

```
admin> ftp -s 1.1.1.1 60.60.60.1
220 dsl-snmp FTP server (SunOS 5.6) ready.
Name:mmahendra
331 Password required for mmahendra.
Password:
230 User mmahendra logged in.
```

The following command specifies a source IP address of 1.1.1.1:

```
ftp> set -s 1.1.1.1
Source IP Address set to : 1.1.1.1
ftp> open 60.60.60.1
220 dsl-snmp FTP server (SunOS 5.6) ready.
Name:mmahendra
331 Password required for mmahendra.
Password:
230 User mmahendra logged in.
```

FTP client URL interface

The URL interface to the TAOS FTP client is based on the interface defined in RFC 1738, *Uniform Resource Locators (URLs)*. With the TAOS implementation, the colon is replaced with a space after `ftp`, and includes a local directory name. You can use the URLs in file transfer scripts.

To use the FTP protocol to transfer a file, place a URL with the following syntax in your Stinger command line:

**`ftp [`*`options`*`] //`*`username`*`:`*`password`*`@`*`hostname`*`:`*`port`*`/`*`url-path`*`/`*`filename`*`;type=a|i `*`local-dir`*

For details about the preceding syntax, see the *Stinger Reference*.

Username and password details

If a username or password includes any of the following characters, you must encode them using the hex values listed in the table that follows.

Character	Hex value
Slash (/)	2F
At sign (@)	40 (forty)
Colon (:)	3A
Semi-colon (;)	3B

Note All hex values need to be proceeded by a percent (%) symbol in the URL, for example, %2F, %3A.

To specify *no* username or password, enter the URL with no characters between the double slash (//) and the hostname. For example:

```
ftp //host.com
```

To specify an *empty* username (rather than no username) and no password, enter the URL with an *at* (@) sign between the double slash and the hostname. For example:

```
ftp //@host.com
```

Note An internal FTP server may not require the user to enter a username, or password.

To specify a username and an empty password, enter the URL with the username followed by a colon and an *at* sign. For example:

```
ftp //samwise:@host.com
```

URL path details

The URL path actually includes the following FTP URL elements:

url-path/filename;type=a|i

If any directory within the URL path contains a slash (/) or semicolon (;), you must encode them.

To represent a slash, use the following code:

```
%2F
```

For example, the following URL transfers via FTP file `motd` from URL path `/etc` on remote system `host.com`:

```
ftp //host.com/%2Fetc/motd
```

Typical FTP URLs

The following examples show how to transfer files by means of URLs.

Sample FTP URL with complete syntax

The following URL performs the following tasks:

```
ftp //foo:bar@135.254.196.191/%2Fhome%2Ftest/ftptest.txt;type=a current
```

1. Changes the directory on the Stinger unit to `current` in the first PCMCIA slot with a FAT-formatted flash card
2. Opens an FTP session with host 135.254.196.191
3. Logs in with username `foo` and password `bar`
4. Changes the remote system's directory to `/home/test/`
5. Switches to ASCII mode
6. Downloads file `ftptest.txt` to `current`
7. Exits FTP

Sample FTP URL with no URL path or local directory

The following URL performs the following tasks:

```
ftp //foo:bar@135.254.196.191//ftptest.txt;type=a
```

1. Opens an FTP session with host 135.254.196.191
2. Logs in with username `foo` and password `bar`
3. Switches to ASCII mode
4. Downloads file `ftptest.txt` to the `root` directory of the first PCMCIA slot that contains a FAT-formatted flash card on the Stinger unit

5 Exits FTP

Sample FTP URL with no username or password

This URL performs the following tasks:

`ftp //@135.254.196.191/%2Fhome%2Ftest/stngrcm.ffs;type=i current`

1 Changes the directory on the Stinger unit to `current` in the first PCMCIA slot with a FAT-formatted flash card

2 Opens an FTP session with host 135.254.196.191

3 Logs in, prompting for a username and password

4 Changes the remote system's directory to `/home/test/`

5 Switches to binary mode

6 Downloads file `stngrcm.ffs` to `current`

7 Exits FTP

Sample FTP URL by specifying a source IP Address

The following URL performs the following tasks:

`ftp -s 1.1.1.1 //foo:bar@60.60.60.1/%2Ftmp%2Ftest/testfile;type=i`

1 Sets the source IP Address to 1.1.1.1

2 Opens an FTP session with host 60.60.60.1

3 Logs in with username `foo` and password `bar`

4 Changes the remote system's directory to `/tmp/test/`

5 Switches to BINARY mode

6 Downloads file `testfile`

7 Exits FTP

Retaining configuration information after clearing NVRAM

You can store minimal system configuration information in a file called `default.cfg` to enable the system to start up with some configuration information, even after you issue the `nvram` command. This feature enables setups with requirements for inband management to clear nonvolatile RAM (NVRAM) and restart the Stinger unit with minimal configuration, such as Ethernet and some ATM connections, so that inband management can proceed.

How it works

You save the system IP address and other basic configuration that you would like to be restored for your system to the `default.cfg` file. You must save the `default.cfg` file to `root directory` or to `root directory/current` in flash memory. After you issue the `nvram` command, the system reboots the control module(s) and looks to NVRAM for configuration information.

The system looks for the `default.cfg` file in the flash directories of the control module in following order:

1 `root directory/`

```
2   root directory/current
```

On a redundant Stinger unit, the system looks for the `default.cfg` file only in the primary control module. If the system finds a `default.cfg` file, it loads the saved configuration to NVRAM and then restarts with the configuration information that was saved to the `default.cfg` file. If you save more than one `default.cfg` file in the flash directories, the software processes the first `default.cfg` file that it finds based on the order listed earlier in this section. If the system finds no `default.cfg` file, then no configuration file is loaded from flash and the system restarts without any configuration.

On Stinger units with dual control modules, you can issue the `nvram` command from the primary control module only.

Note You must upgrade both the control module boot code and the control module software to the current software version to use the `default.cfg` feature.

Loading a `default.cfg` file from the TFTP server

The following sample command loads a `default.cfg` file from the TFTP server to the primary controller and then transfers a copy to the secondary control module:

```
admin> load file network IPaddress default.cfg
loading code from IPaddress
file default.cfg...
done.
Attempting to write image(s) to other controller
Trying device 1 of remote controller first
Transferring 1/current/default.cfg ...
done.
1 image successfully transferred
```

On a redundant system, depending on the software version your Stinger unit is running, the system automatically copies the `default.cfg` from the primary control module to the secondary control module.

Verifying that the default.cfg is saved to the desired directories

Use the `ls` command to verify that you have successfully saved the `default.cfg` file to the desired directories on the control modules.

On the primary control module, enter the `ls` command. For example:

```
admin> ls
Controller { first-control-module } ( SECONDARY ):
                                Reqd  Oper   Slot Type
    { second-control-module }    UP    UP     ( PRIMARY )
Slot state information is not available for secondary controller
admin> ls
ls Flash card 1:
/:
  current/                        0 Tue Sep 24 22:27:14 2002
/current:
  stngrima.ffs              872522 Wed Jul 23  9:39:18 2003 Version 9.5-206.0
  stngrcm2.ffs             4827612 Wed Jul 23  9:40:42 2003 Version 9.5-206.0
  stngrctdmt72.ffs         1136044 Wed Jul 23  9:41:22 2003 Version 9.5-206.0
```

```
  stngrshdsl.ffs          1114989 Wed Jul 23  9:41:02 2003 Version 9.5-206.0
  config                   340926 Fri Nov 15 16:09:38 2002
  stngrrsdsl.ffs           988688 Wed Jul 23  9:39:04 2003 Version 9.5-206.0
  cm2_trap.ffs            4782094 Mon May 12  0:18:10 2003 Version 9.5-206.0
  cm_0617_2.ffs           4439012 Tue Jun 17 17:48:24 2003 Version 9.5-206.0
  default.cfg                 292 Wed Jul 17 22:11:12 2003

Total space:   31997952 bytes
       used:   30900224 bytes
       free:    1097728 bytes
```

On a redundant system, open a session with the secondary control module and enter the `ls` command. Verify that the `default.cfg` file has been saved to the desired directories. In the following example, the primary control module is in slot 8 and the secondary control module is in slot 9.

admin> **open 1 9**

```
admin> ls
ls Flash card 1:
/:
  current/                      0 Wed Apr  7 18:47:34 2004
/current:
  stngrima.ffs             872522 Wed Jul 23  9:38:04 2003 Version 9.5-206.0
  stngrcm2.ffs            4827612 Wed Jul 23  9:37:26 2003 Version 9.5-206.0
  stngrctdmt72.ffs        1136044 Wed Jul 23  9:38:24 2003 Version 9.5-206.0
  stngrshdsl.ffs          1114989 Wed Jul 23  9:38:44 2003 Version 9.5-206.0
  stngrrsdsl.ffs           988688 Wed Jul 23  9:37:50 2003 Version 9.5-206.0
  default.cfg                292 Wed Jul 16 22:11:12 2003

Total space:   31997952 bytes
       used:   19693568 bytes
       free:   12304384 bytes
```

Note If the `default.cfg` file has not been saved to the flash memory of the secondary control module, use the `loadmate` command to copy the `default.cfg` file from one control module to another.

For example, to copy the `default.cfg` from PCMCIA flash card 1 of the primary control module to flash card 1 of the secondary control module, enter the following command from the primary control module:

admin> **loadmate file 1 1 /current/default.cfg**

Enter the `ls` command from the secondary control module to verify that the `default.cfg` file has been saved to the desired directories on the secondary module.

What happens after you issue the `nvram` command on a unit with a `default.cfg` file

Note After you issue the `nvram` command, the system undergoes two reboot cycles.

If the system detects a default configuration after an `nvram` command, it displays the following sample message:

```
******  WARNING ***** WARNING ****** WARNING ****** WARNING ******* WARNING
   System Integrity checking in restoring from default.cfg will take
   a few minutes. User must not make changes to system profile(s) at
```

```
   this time.
******  WARNING ***** WARNING ****** WARNING ****** WARNING ******* WARNING
configuration being restored from flash file 1/current/default.cfg...
configuration loaded from flash.
```

Using extended profiling

One 128KB segment of onboard flash memory that was previously reserved for the boot image can now be made available for storing configuration profiles. Extending the amount of memory used for profiles is referred to as *extended profiling.* When this feature is enabled, twice as many configured profiles can be stored in nonvolatile RAM (NVRAM).

Requirements and limitations

The system requires a 32MB PCMCIA flash memory card to use extended profiling.

Once you have enabled extended profiling, you cannot restore the system's configuration to an earlier software version that does not support extended profiling if the configuration file is larger than one segment (128KB). If you must restore the current configuration to an earlier software version, see "Restoring an earlier configuration after enabling extended profiling" on page 1-33.

Caution Before enabling extended profiling, you must complete the entire upgrade process so that both the boot loader and the control module images support extended profiling. If you enable the feature while one of these images is at a version level that does not support extended profiling, *all profile information will be lost.*

Enabling extended profiling

To use extended profiling, follow these steps:

1. Verify that the system has a 32MB PCMCIA flash memory card installed.
2. Upgrade to the current TAOS version. (See the release note for the version you are upgrading to.)
3. Use the `nvram -u` command to verify that the system can now support extended profiling. (A message indicating that extended profiles is not in use appears.)

   ```
   admin> nvram -u
   Not Using Extended profiles
   NVRAM seg[0]:start 1000C028 size 131064 avail 117904 used 13160 cmpct 0
   ```

4. Use the `nvram -e` command to enable extended profiling on the primary and secondary control modules:

   ```
   admin> nvram -e
   ```

   The system displays the following messages and a prompt:

   ```
   Respond to the prompt as appropriate. To leave the system unchanged, type
   n. To enable extended profiling (which causes a reset), type y.
   ```

5. After the reset, use the `nvram -u` command to verify that the system is now using extended profiles.

   Two memory segments are now available for profile storage.

Restoring an earlier configuration after enabling extended profiling

Because software releases are not necessarily backward compatible, Lucent Technologies recommends that you restore a backup configuration made under the earlier software version or one of its predecessors.

To downgrade to an earlier software version after enabling extended profiling, follow these steps:

1 Save the configuration to another system. For example:

```
admin> save network 10.10.10.10 cfgsave
```

2 Reformat NVRAM.

```
admin> nvram -f
```

When you clear NVRAM, the system loses its IP addresses.

3 After reformatting NVRAM, perform the following steps to regain a minimal IP configuration:

- In the IP-Interface profiles, set the IP addresses of the system's Ethernet ports.
- Reset the system for these changes to take effect.

4 Load the earlier version of the boot loader. For example:

```
admin> load boot-sr network 10.10.10.10 stgsrb.bin
```

5 Load the earlier version of the tar file. For example:

```
admin> load tar network 10.10.10.10 stgrel.tar
```

6 Reset the system.

7 Restore a backup configuration made under the restored software version or one of its predecessors.

Using a script to configure a Stinger unit

The TAOS command-line interface allows you to create configuration scripts with a simple text editor and a Telnet client program with a Text Upload feature. This section briefly describes how you can use a script to make changes to the Stinger configuration.

Following are the basic steps:

1 Create a text file that contains the configuration commands as you normally enter them in the TAOS command-line interface.

2 Log into the Stinger unit with sufficient permissions to change the configuration.

3 To upload the file to the Stinger unit, use the upload file feature of your Telnet terminal software.

Following is an example of a text file that configures an SDSL line in shelf 1, slot 7:

```
new SDSL
set name = SF
set physical-address shelf = {shelf-1 slot-7 1 }
set enabled = yes
set line-config = { 0 1 static { any-shelf any-slot 0 } singlebaud 784000 coe
}
```

```
write -f
;
```

Note The `write -f` command causes the script to overwrite an existing configuration without prompting.

You can use this file as a basis for configuring all 28 lines on a DS3-ATM trunk module by changing the parameters, such as Item-Number, as required. Carefully review your text file to make sure it is correct.

Use an ASCII text upload to upload the text file directly to the Stinger unit prompt. Carefully review your changes through the console.

Timing the saving of profiles

You can configure the system to pause before it executes the next command-line interface command. This feature is useful for provisioning connection profiles using the NavisAccess™ management software. It enables the system to completely delete an old configuration profile before using a new profile with the same name.

The `sleep` command specifies the number of seconds the system pauses before it executes the next command. You can specify a value between `0` and `60` seconds. The default setting is `5` seconds. NavisAccess™ management software users can introduce this command in a configuration file sent to a Stinger unit to time the saving of configuration profiles.

The syntax of the sleep command is as follows:

`sleep` ***`[seconds]`***

From the command-line interface, the following sample command configures the system to pause for 10 seconds before it executes the next command-line interface command:

admin> **sleep 10**

Reloading profiles from RADIUS

Use the `refresh` command to open a connection to a RADIUS server and retrieve the latest configuration information. For syntax information, see the *Stinger Reference*.

When you use the `-n` option, the Stinger unit requests a reload of all nailed profiles from the RADIUS server:

```
admin> refresh -n
```

You can specify how dedicated (nailed) connections are handled following an entry of `refresh -n` by using the `perm-conn-upd-mode` parameter in the `system` profile:

- If `perm-conn-upd-mode` is set to `all` (the default), all existing permanent connections are broken and then reestablished (along with any new connections) following the update. This setting causes a service interruption every time any nailed profile is updated or added.
- If `perm-conn-upd-mode` is set to `changed`, only new connections are created, and only those with modified attribute values are reestablished.

Resetting the unit

When you reset the Stinger unit, it restarts and terminates all active connections. All users are logged out, and the default security level is reactivated. In addition, a system reset can cause a WAN line to temporarily shut down due to momentary loss of signaling or framing information. After a reset, the Stinger unit runs power-on self tests (POSTs).

By default, entering the `reset` command without any arguments resets each control module. To reset the Stinger with confirmation, proceed as follows:

```
admin> reset
Reboot the entire system, dropping all connections? [y/n]
```

In a redundant system, reset the secondary control module only with no confirmation:

```
admin> reset -f -r secondary_controller
Please standby. System reset in progress.
```

See the *Stinger Reference* for additional command options.

Managing PCMCIA flash cards

Each control module on a Stinger FS, Stinger FS+, Stinger LS, and Stinger RT unit supports up to two PCMCIA flash memory cards. The Stinger MRT chassis contains built-in flash memory. Currently, the flash cards contain code for the modules and the control module. The system configuration is stored in the onboard NVRAM. (See "Managing system configuration" on page 1-20.)

To access a specific control module, you can either telnet to its configured IP address or connect by way of the control module's serial port. Once you have connected to the control module, you must consider if you need to format a flash card or flash memory, display its contents, or check the file system.

Formatting a flash card

Before using a PCMCIA flash card in the Stinger unit, you must format it. First insert the card into slot 1 or slot 2 in the control module, then use the `format` command. Following are examples of formatting the card in slot 1:

```
admin> format flash-card-1
```

or

```
admin> format 1
```

For details of the command-line options for the `format` command, see the *Stinger Reference*.

Displaying the contents of flash

To check the Stinger module images stored in the flash card code directory, use the `dircode` command, as shown in the following example:

```
admin> dircode
Card 1, format FAT, capacity 30MB
/current:
  ima-24t1-card             872522 Wed Jul 23  9:38:04 2003 Version 9.5-206.0
```

```
  cm-v2                   4827612 Wed Jul 23  9:37:26 2003 Version 9.5-206.0
  stngr-72-ct-adsl-card   1136044 Wed Jul 23  9:38:24 2003 Version 9.5-206.0
  shdsl-card              1114989 Wed Jul 23  9:38:44 2003 Version 9.5-206.0
  sdsl-atm-v2-card         988688 Wed Jul 23  9:37:50 2003 Version 9.5-206.0

Total space:   31997952 bytes
       used:   19693568 bytes
       free:   12304384 bytes
```

The information displayed by this command includes the flash card number (1 or 2) and the size of the code directory. It also shows the following information about each code module:

- Type of Stinger module supported
- Size of the code
- Date the code was loaded to the flash card or flash memory
- Code version

Checking the file system

If the `dircode` command shows a code status other than `good` or if you suspect inconsistencies in the flash card files, use the `fsck` command to check the code directory. The `fsck` command checks inconsistent conditions in the code directory as well as file contents on a PCMCIA flash card or flash memory.

If errors are detected, they are reported but not fixed. If the `fsck` command reports errors, you must reformat the flash card and then load the code again. If necessary, download the code file again from the Lucent Technologies FTP server.

To check the file system on the flash card in PCMCIA slot 1, or built-in flash memory, use the `fsck` command as shown in the following example:

```
admin> fsck 1
Volume Stats:
    Block Size: 512 (typical: 512)
    Blocks Per Cluster: 4 (typical: 1, may be powers of 2 up to 16)
    Reserved Blocks: 1 (typical: 1, but may be 0 - hundreds)
    Number of FATs: 2 (must be 2)
    Number of Root Directory Entries: 128 (typically betwn 32 and 224)
    Total Blocks: 13824
    Media Descriptor: f0 (ignored)
Volume Info calculated from values above:
    Blocks Per Fat: 11
    Fat Start Block: 1
    Root Dir Start Block: 23
    Data Start Block: 31
    Number of Root Dir Blocks: 8
    Number of Clusters: 3448
    FAT Type: Fat12
Cluster Usage
    Usable Clusters: 3446
    Free Clusters: 3446
    Clusters lost during interrupted writes: 0
    Other reserved clusters: 0
```

For details of the command-line options for the `fsck` command, see the *Stinger Reference*.

Using the status window

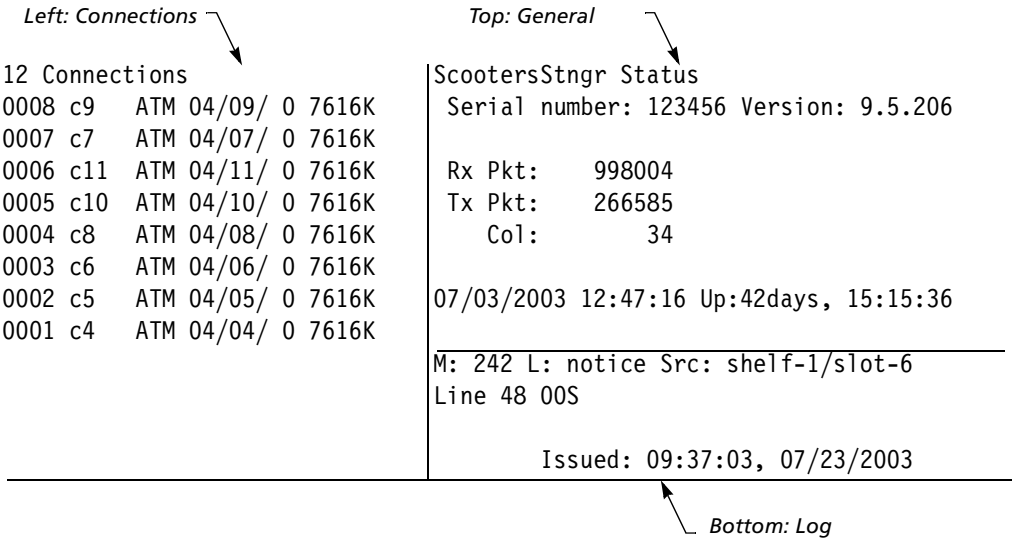
You can use a status window to display the continuous stream of statistics that the Stinger unit generates about its activities. For example, one status window displays up to 100 of the most recent system events that have occurred since the Stinger unit was started up, and another displays statistics about the currently active session. A VT100 window that can accommodate an image of at least 80 columns by 24 rows is required for displaying the status screens.

Displaying the status window

You can open the status window using the `status`, `connection`, `line`, `view`, or `log` command. For details about using these commands, see the *Stinger Reference*.

To open the system status window, enter the `status` command. Figure 1-1 shows the sample contents for each area of the status window.

Figure 1-1. Sample contents of a status window



The system prompt moves to just below the status window. If the system prompt is not visible below the status window, press Escape to display it.

To close the status window, enter the `status` command again:

```
admin> status
```

Understanding the status window

Figure 1-1 shows the main areas of the status window. In its default configuration, these areas contain the following information:

- Left—Connection information is displayed on the left side of the window.
- Top—General information, such as serial number, software version, and uptime are displayed in the upper right side of the window.

- Bottom—Log information is displayed in the lower right side of the window.

Connection status information

With the default settings in a `user` profile, the left area of the status window initially displays connection information, as shown in Figure 1-1. Each line represents an active connection; its username or station name; the type of connection; the shelf, line, and channel (separated by slashes) on which the call was placed or received; and the bandwidth or baud rate of the connection.

If the status window is not already visible, the `connection` command opens it with the connection-status information displayed:

```
admin> connection
```

This command puts the window in connection-status mode, with the following message displayed below the status window:

```
[Next/Last Conn: <dn/up arw>, Next/Last Page: <pg dn/up>, Exit: <esc>]
```

This message indicates the keystroke sequences you can use for displaying additional information in the connection-status area. The Down Arrow and Up Arrow keys display the next and previous connections, respectively, in the list of active connections. The Page Down and Page Up keys display the list, one screen at a time.

When the `connection-status-mode` message is displayed, the system prompt does not appear at the bottom of the window. Press the Escape key to exit this mode and return to the system prompt.

General status information

With the default settings in a `user` profile, the top area of the status window initially displays general status information about the Stinger unit, including its serial number, the version of system software that the unit is running, and the number of packets transmitted and received. This area also shows the current system date and time and how long the system has been operational.

If the top of the status window is displaying another kind of information, you can redisplay the general status information with the `view` command:

```
admin> view top general
```

Line and channel status

To display information about WAN lines and channels, use the `line` command. Because space is limited for this graphical display of status information about lines and channels, the line-status window uses identifiers and codes. For example, the line's link status uses a two-character code such as LA (link active), RA (Red Alarm), YA (Yellow Alarm), and so forth. For complete information on line-status codes, see the *Stinger Reference*.

If the status window is not already displayed, the following `line` command opens it with line-status information displayed in the bottom (lower right) of the window:

```
admin> line
```

Or, you can use the following command to specify that the line-status information appears in the top of the window, replacing the general status information:

```
admin> line top
```

You can display information about all lines installed in the system if you wish, but the default is to show information only about enabled lines. To display the status of all lines, enter the following command:

```
admin> line all
```

When you enter the `line` command, the system puts the window in line-status mode and displays the following message, which indicates the key sequences for displaying additional information in the line-status area:

```
[Next/Last Line: <dn/up arw>, Next/Last Page: <pg dn/up>, Exit: <esc>]
```

The Down Arrow and Up Arrow keys display the next and previous lines, respectively, in the list. The Page Down and Page Up keys display the list a screen at a time.

Line status information includes the following identifiers and codes:

- Line identifier in *shelf/slot/line* format
- Two-character code indicating the line's link status
- Single-character code indicating channel status
- Single-character code indicating channel type

For additional information about identifiers and codes, see the *Stinger Reference*.

When the line-status-mode message is displayed, the system prompt does not appear at the bottom of the window. Press the Escape key to exit this mode and return to the system prompt.

Log message information

With the default settings in a `user` profile, the bottom area of the status window initially displays the most recent message from the Stinger log buffer. The number of system event messages stored in the log is set by the `save-number` parameter in the `log` profile.

The first line of the event log window shows the log entry number (M: 00 through M: *N*, where *N* is set in the `save-number` parameter of the `log` profile), the level of message, and the device on which the event occurred. The last line shows the date and time when the event occurred.

The middle of the window displays the text of the most recent message.

If the status window is not already displayed or if you want to scroll through the log, use the `log` command:

```
admin> log
```

If the Status window is not displayed, the `log` command opens it and displays the log-mode message below the Status window. (If the Status window is already open, the `log` command just displays the message.)

```
[Next/Last Conn:<dn/up arw>, Next/Last Page:<pg dn/up>,Exit: <esc>]
```

This message indicates the key sequences you can use for displaying additional information in the Log area:

- The Down Arrow and Up Arrow keys display the next and previous messages in the buffer, respectively.

- The Page Up and Page Down keys display the first and last messages in the buffer, respectively.

When the log-mode message is displayed, the system prompt does not appear at the bottom of the window. Press the Escape key to exit this mode and return to the system prompt.

Customizing the status window display

You use the `user` profile to specify whether these statistics are always displayed when a user logs in using that profile, the areas of the window that are displayed by default, and the size of the status windows.

The following parameters in a `user` profile, shown with their default values, specify the contents of the status window:

```
left-status = connection-list
top-status = general-info
bottom-status = log-window
```

The following parameters in a `user` profile, shown with their default values, specify the size of the status window. The `status-length` parameter must be at least 6 lines smaller than `screen-length`.

```
screen-length = 24
status-length = 18
```

See the *Stinger Reference* for details about these parameters.

The following commands configure the `user` profile to display the status window after login, and to show line information in the bottom area of the window. This set of commands also configures a larger terminal emulator window and status screens.

```
admin> read user test
USER/test read
admin> set default-status = yes
admin> set bottom-status = line-status
admin> set screen-length = 36
admin> set status-length = 30
admin> write
USER/test written
```

Changing current status window sizes

The `screen` command enables you to change the size of the terminal emulator and status windows for the current session. For syntax information, see the *Stinger Reference*.

The following example changes the current display size to 55 lines long and 100 characters wide:

```
admin> screen 55 -w 100
```

If the Status window is open when you enter the `screen` command, the command resizes it dynamically. If it is not open, the Status window is resized when you next open it.

Displaying basic system information

The following sections describe how to display basic system information such as hardware platform, system name, serial number, software version, boot firmware version, control module role, control module revision and model number, system and module uptime.

Displaying system hardware information and software version

The system-level command `info` displays information about the Stinger system, including hardware platform, system name, serial number, software version, boot firmware version, and control module role.

During system reboot, if you are connected to the control module console port, the system displays the platform type and the TAOS version running on the system.

```
admin> info
Platform         : Lucent Stinger LS/RT - 23"
System Name      : stinger
Serial Number    : 11178242
Software Version : TAOS 9.5-206.0 (stngrcm2)
                   * * * rtr/stngrcm2 <mmahendra> Mar 04 2003 * * *
Boot Version     : TAOS 9.5-206.0
Controller Role  : Primary
Hardware revision: 2.0  Model A
```

The fields displayed by the `info` command are defined as follows:

Field	Definition
`Platform`	Hardware platform type. This field reports one of the following values: ■ Lucent Stinger MRT - 23" ■ Lucent Stinger MRT - 19" ■ Lucent Stinger LS/RT - 23" ■ Lucent Stinger LS/RT - 19" ■ Lucent Stinger FS ■ Lucent Stinger FS+ On a redundant system, if you enter the info command from the secondary control module, this field shows `Lucent Stinger`.
`System name`	Name of the system as configured in the `system` profile. If the `system` profile has not been configured, the command displays `(not configured)`.
`Serial number`	Serial number of the control module on which you entered the command.
`Software version`	Current version of TAOS.
`Boot version`	Version of boot loader on the system.
`Controller role`	Current role of the control module, either primary or secondary.

Field	Definition
Hardware revision	Revision number of the control module on which you entered the command.

System and module uptime

The `uptime` command reports how long the system and its individual modules have been operating. Without an argument, the command displays system uptime. For example, on the a Stinger FS, Stinger FS+, Stinger LS, or Stinger RT unit:

```
admin> uptime
12:53:37
{ shelf-1 first-control-module } cm-v2   0 days 18:58:57 (PRIMARY)
```

On a Stinger MRT:

```
admin> uptime
11:47:04
{ shelf-1 first-control-module } mrt-cm 0 days 01:12:07 9.5-206.0
```

If you specify a slot and shelf number, the `uptime` command displays the current time; identifies the module installed in the slot, and the length of time that the module installed in the slot has been operating. The following example shows that an SDSL LIM in slot 3 has been operating for 48 minutes and 38 seconds:

```
admin> uptime 1 3
16:15:06
{ shelf-1 slot-3 }     sdsl-atm-card    0 days 00:48:38 9.5-206.0
```

If you use the `-a` option, the command displays the uptime only for modules in the UP state. For example:

```
admin> uptime -a
16:08:37
{shelf-1 slot-2 }        sdsl-atm-card   0 days 00:42:09 9.5-206.0
{shelf-1 slot-4 }  al-dmtadsl-atm-card   0 days 00:42:09 9.1-142.0
{shelf-1 control-module} shelf-controller  0 days 00:43:26 9.0-126.0
```

Software version

The `version` command shows the TAOS version installed, the hardware version of the control module, or the model number of the control module on which you entered the command.

For example, on a Stinger FS, Stinger FS+, Stinger RT, or Stinger LS unit

```
admin> version
Software version 9.5-206.0
* * * tram206/stngrcm2 <arajagop> Jul 17 2003 09:49 * * *
Hardware revision: 2.0  Model A
```

If no hardware revision number is displayed, the Stinger FS, Stinger FS+, Stinger RT, or Stinger LS unit is installed with a revision 1 control module and it is running a version of TAOS prior to TAOS 9.1-142. The Stinger unit displays the model number of the control modules only for revision 2 or higher control modules.

On a Stinger MRT, the `version` command displays the software version and the hardware revision number of the Stinger MRT. For example:

```
admin> version
Software version 9.5-206.0
* * * rtr/stngrcm2 <vasanthaku> Jul 9 2003 17:33 * * *
Hardware revision: 2.2  Model E - IP with gigE fiber interface.
```

You can also use the `get` command to display the setting for the `software-version` parameter in the `slot-info` profile. For example:

```
admin> get slot-info {1 8 0} software-version
[in SLOT-INFO/{ shelf-1 first-control-module 0 }:software-version]
software-version = 9.5-206.0
```

Serial number

The serial number of a Stinger unit is the serial number of one of its control modules. The `serial-number` parameter in the `base` profile or a control module's `slot-info` profile defines the serial number value.

To display the serial number of a Stinger unit, use the `get` command to show the setting of the `serial-number` parameter. For example, to display the serial number using the `base` profile:

```
admin> get base serial-number
[in BASE:serial-number]
serial-number = 555xx115
```

To display the serial number from control module in slot 8:

```
admin> get slot-info {1 8 0} serial-number
[in SLOT-INFO/{ shelf-1 first-control-module 0 }:serial-number]
\serial-number = 555xx115
```

You can also use the `revision` command to display the serial number of a control module. However, it requires debug authorization. For example:

```
admin> revision
first-control-module : revision = 0 1 10 555xx115
```

Displaying the boot-loader version

The `boot-cm-version` parameter in the `system` profile displays the version of the current boot-loader (the *xxx*`.bin` file). The boot-loader updates the value of this parameter with its version at every system reset. Following is a sample of this profile:

```
admin> get system boot-cm-version
[in SYSTEM:boot-cm-version]
boot-cm-version = 9.5-206.0
```

Viewing the factory configuration

The read-only `base` profile displays software version, enabled features (software licenses), network interfaces, and other system information that is not modified across resets. These values are read from the system ROM, security program array logic (PAL), and the hardware assembly itself. For information about the parameters in the `base` profile, see the *Stinger Reference*.

To view the `base` profile, use the `get` command. For example:

```
admin> get base
[in BASE]
shelf-number = 1
software-version = 9
software-revision = 5
software-level = ""
manufacturer = dba-ascend-mfg
d-channel-enabled = yes
aim-enabled = yes
switched-enabled = yes
multi-rate-enabled = yes
t1-pri-conversion-enabled = yes
frame-relay-enabled = yes
maxlink-client-enabled = enabled
data-call-enabled = yes
serial-number = 55555072
hardware-level = 0
countries-enabled = 511
domestic-enabled = yes
phs-2-1-support = no
firewalls-enabled = yes
network-management-enabled = yes
phs-support = no
routing-protocols-disabled = no
tnt-adsl-restricted = yes
tnt-sdsl-restricted = yes
tnt-idsl-restricted = yes
ss7asg = disabled
atmp-enabled = enabled
l2tp-enabled = enabled
pptp-enabled = enabled
l2f-enabled = enabled
sdtn-enabled = disabled
vrouter-enabled = enabled
v110-enabled = enabled
network-mgmt-voip-enabled = yes
wormarq-enabled = disabled
nm-copper-loop-test-enabled = yes
nm-reporting-enabled = yes
nm-vpn-enabled = yes
nm-navis-radius-enabled = yes
restrict-redundancy-enabled = no
pnni-enabled = yes
ima-enabled = yes
intra-trunk-connections-enabled = yes
aps-enabled = yes
nm-prov = yes
nm-prov-core = yes
ras-enabled = yes
h248 = no
```

Managing administrative connections

You can use the `userstat`, `view left session`, or `who` command to display connection information for users.

Displaying administrative session information with the userstat command

To display the most complete information about active sessions, use `userstat` with the `-l` option, as in the following example:

```
admin> userstat -l
SessionID  Line/Chan   Slot:Item   Tx/Rx Rate  Svc Address   Username
ConnTime   IdleTime   Dialed#
383578461  1.17.02/002 1:17:02/002  155M/ 155M ATM 0.0.0.0
sig-17-2-0-5
32:21:18   unknown
383578460  1.17.03/002 1:17:03/002   44M/  44M ATM 0.0.0.0
rcc-17-3-0-18
32:21:18   unknown
383578459  1.17.03/001 1:17:03/001   44M/  44M ATM 0.0.0.0
sig-17-3-0-5
32:21:19   unknown
383578458  1.17.02/001 1:17:02/001  155M/ 155M ATM 0.0.0.0
rcc-17-2-0-18
32:21:27   unknown
<end user list>  4 active user(s)
```

Following are the `userstat` output fields with descriptions:

Field	Description
`Sessionid`	Unique ID assigned to the session.
`Line/Chan`	Physical address (*shelf.slot.line/channel*) of the network port on which the connection was established.
`Slot:Item`	*Shelf:slot:item/logical-item* of the host port to which the call was routed.
`Tx/Rx Rate`	Transmit and receive rate.
`Svc`	Type of service in use for the session. Following are the possible values: ■ `---` The service is being negotiated.) ■ `TLN` Telnet ■ `BTN` Binary Telnet ■ `ATM` Asynchronous Transfer Mode
`Address`	IP address of the user.
`Username`	Name of the user.
`ConnTime`	The amount of time (in hours:minutes:seconds format) since the session was established. This field appears only with the `-l` option.

Field	Description
IdleTime	The amount of time (in *hours:minutes:seconds* format) since data was last transmitted across the connection. This field appears only with the -l option.
Dialed#	The number dialed to initiate this session.

Customizing the output of the userstat command

The -o option with one or more format specifiers can limit the commands's output to those fields of interest. For example, if you use the -o option and indicate the codes for session ID and line or channel information, the command shows only the following details:

```
admin> userstat -o %i %l
SessionID  Line/Chan
288532030  1.01.01/012
<end user list>  1 active user(s)
```

For definitions of the available specifiers, see the *Stinger Reference*.

Displaying information related to a known IP address

Use the userstat -a command to display information related to a known IP address. The userstat -a command requires an IP address argument on the command line. For example:

```
admin> userstat -a 1.1.1.238
SessionID  Line/Chan   Slot:Item   Tx/Rx Rate  Svc Address    Username
288532030  1.01.01/012  1:03:01/002 56000/56000  PPP 1.1.1.238  net1
<end user list>  1 active user(s)
```

To display only the relevant username, include the -o option as follows:

```
admin> userstat -a 1.1.1.238 -o %u
Username
net1
<end user list>  1 active user(s)
```

Displaying information related to a known username

Use the userstat -u command to display information related to a known username. You must enter a username argument on the command line. For example:

```
admin> userstat -u net1
SessionID  Line/Chan   Slot:Item   Tx/Rx Rate  Svc Address    Username
288532030  1.01.01/012  1:03:01/002 56000/56000  PPP 1.1.1.238  net1
<end user list>  1 active user(s)
```

To display only the user's IP address, include the -o option as follows:

```
admin> userstat -u net1 -o %a
Address
1.1.1.238
<end user list>  1 active user(s)
```

Using the `view left session` command

To display information about administrative users, including user name and source IP address, use the `view left session` command. For example:

```
admin> view left session
Sessions                    x Status
admin     console           x Serial number: 1934589598Version: 9.5-206.0
admin     192.11.157.169    x
admin     192.11.157.132    x  Rx Pkt:     539601
admin     192.11.157.132    x  Tx Pkt:       6744
                            x     Col:          0
                            x
                            x07/21/2003  22:02:34   Up:    4 days, 12:14:23
                           xqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
                           xM: 23  L: notice  Src: shelf-1/first-control-mo
le                          x
                            x Line 18.2 down
                            x
                            x
                            x
                            x
                            x                Issued: 09:48:50, 07/17/2003
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
```

The Sessions section shows the user name and source IP address of administrative users from Telnet sessions. An asterisk (*) denotes the current session.

Displaying administrative users

The `who` command displays names of administrative users, `user` profiles, and IP addresses of administrative users from Telnet sessions. An asterisk (*) denotes the current session. For example:

```
admin> who
  user                   profile                from
                         super                  console
* admin                  admin                  135.254.196.37
  pratul                 admin                  135.254.196.37
```

Terminating a user connection

To terminate a user connection, use the `userstat -k` command, as in the following example:

```
admin> userstat
SessionID Line/Chan  Slot:Item   Rate  Svc Address        Username
332429649 1.13.01/000 1:13:01/000 3360/3360 ATM 1.1.1.1 11-0-13
<end user list>  1 active user(s)

admin> userstat -k 332429649
Session 246986325 cleared
```

The `userstat` command can terminate Telnet, Telnet binary, Raw TCP, or terminal server user sessions.

You can also terminate an administrative session using the `who -k` command. The

`who -k` command requires System privileges. For example, the following command disconnects the user `pratul` logged in from IP address 135.254.96.37:

```
admin> who -k pratul 135.254.196.37
LOG critical, Shelf 1, Controller-1, Time: 05:24:17--user
admin from 135.254.196.37 disconnected user pratul from 135.254.196.37
1 administrative user killed.
```

The `who -k` command disconnects all sessions with the user name `pratul` logged in from IP address `135.254.96.7`.

You cannot use the `who -k` command to disconnect the current session or a session from the console if for its serial port the `user-profile` parameter in the `serial` profile is set to a value other than null.

Disconnecting an idle connection

You can configure a Stinger unit to disconnect a modem connection after a specified period of inactivity. To configure a timeout value, set the `inactivity-time` parameter in the `modem` profile with a value from `0` through `255` seconds. With the default setting of `0`, the timer is disabled and an inactive modem connection is not disconnected after any period of inactivity.

The following sample commands configure the Stinger unit to disconnect a modem connection after it has been inactive for 120 seconds.

```
admin> read modem { shelf-1 first-control-module 3 }
MODEM/{ shelf-1 first-control-module 3 } read

admin> list
[in MODEM/{ shelf-1 first-control-module 3 }]

admin> set inactivity-time = 120

admin> write
MODEM/{ shelf-1 first-control-module 3 } written
```

Working with Stinger Modules 2

For information about how to configure a particular module, see the module guide for your device at `http://www.lucentdocs.com/ins`. For information about managing the Stinger system, see Chapter 1, "Administering a Stinger System."

Understanding physical addressing on Stinger units

On modular Stinger units, the True Access™ Operating System (TAOS) software uses the physical address to provide configuration and administration access to the module's functions. Because TAOS associates module functions with the same slot numbers on all Stinger units, the functions are grouped into *virtual* slots on the Stinger MRT chassis.

Note In this document, *Stinger MRT* refers to both the Stinger MRT 23 and Stinger MRT 19 chassis.

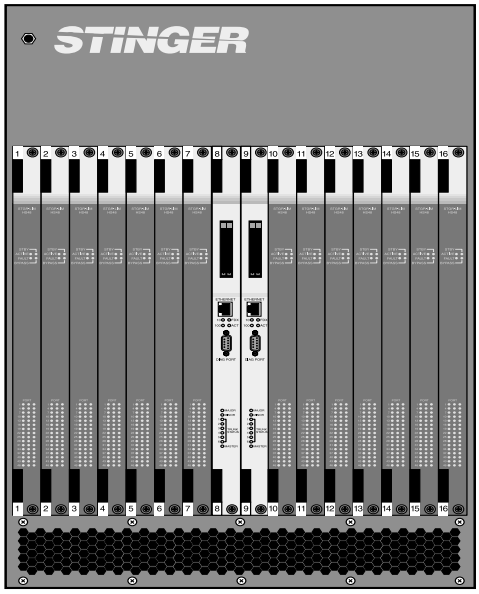
The chassis of Stinger FS, Stinger FS+, Stinger LS, or Stinger RT units have slots that accept plug-in modules with different functions. Each module has a physical address composed of its shelf number, slot number, and item number in the format `{ shelf-1 slot-N item-N }`. The shelf number is always 1.

In contrast, the smaller Stinger MRT units integrate the functions of the control module, line interface modules (LIMs), and line protection modules (LPMs) into the chassis, and have a single trunk module slot.

Figure 2-1 shows the modules on the front panel of a Stinger FS or Stinger FS+ unit. The slots are numbered from left to right, with the middle slots reserved for the

control modules. On a Stinger LS or Stinger RT unit, which has fewer slots, the control modules are on the right.

Figure 2-1. Front panel of a Stinger FS unit



Note On a Stinger MRT, because control module and LIM functions are incorporated into the unit's chassis, the terms *control module* and *LIM* in this guide refer to the control module and LIM functions on the Stinger MRT, and not to physical modules.

Table 2-1 shows how TAOS relates slot numbers to modules and module functions on all Stinger units, for configuration and administration. (LPMs are not configured.)

Table 2-1. How TAOS organizes Stinger module functions

Module type	**Module function(s)**	**Slot numbers on Stinger FS, Stinger FS+, Stinger LS, and Stinger RT units**	***Virtual* slot numbers on Stinger MRT units**
LIM	Connecting the unit to subscriber lines	■ Slots 1 through 7 ■ Slots 10 through 16 (Stinger FS and Stinger FS+ only)	Virtual slot 1
Control module(s)	General control and configuration of the unit	Slots 8 and 9	Virtual slot 8

Table 2-1. How TAOS organizes Stinger module functions

Module type	Module function(s)	Slot numbers on Stinger FS, Stinger FS+, Stinger LS, and Stinger RT units	*Virtual* slot numbers on Stinger MRT units
Trunk module	Connecting the unit to ATM links	Slots 17 and 18	■ Virtual slot 17 (built-in STS-3 interface) ■ Virtual slot 18 (trunk module)

Viewing Stinger modules

You can use the `show` command and `slot-info` profile to display information about the modules installed or configured in the Stinger unit and the status of each module.

Using the `show` command

The `show` command lists the address of each module, its required operating state and current operating state, and its type. For example, on a Stinger FS, Stinger FS+, Stinger LS, or Stinger RT:

```
admin> show
Controller { first-control-module } ( PRIMARY ):
                                Reqd  Oper   Slot Type
{ shelf-1 slot-2 0 }            UP    NONE   stngr-48a-adsl-card
{ shelf-1 slot-3 0 }            UP    UP     al-dmtadsl-atm-card
{ shelf-1 slot-5 0 }            UP    NONE   dadsl-atm-24-card
{ shelf-1 slot-6 0 }            UP    NONE   dadsl-atm-24-card
{ shelf-1 slot-7 0 }            DOWN  RESET  glite-atm-48-card
{ shelf-1 slot-11 0 }           UP    NONE   stngr-48a-adsl-card
{ shelf-1 slot-14 0 }           DOWN  RESET  stngr-48b-adsl-card
{ shelf-1 trunk-module-1 0 } UP    UP     ds3-atm-trunk-daughter-card
```

On an ADSL 36-port Stinger MRT, the `show` command displays the following output:

```
admin> show
Shelf 1 ( standalone ):
                                Reqd  Oper  Slot Type
  { second-control-module }     UP    UP    ( SECONDARY )
  { shelf-1 slot-1 0 }          UP    UP    mrt-36-adsl-card
  { shelf-1 trunk-module-1 0 } UP    UP    oc3-atm-trunk-daughter-card
  { shelf-1 trunk-module-2 0 } UP   UP     oc3-atm-trunk-daughter-card
```

On a unit with dual control modules, the `show` command identifies which control module is primary. The command also lists the addresses of each slot with an

installed module. Table 2-2 describes the values displayed for the Reqd, Oper, and Slot-Type fields.

Table 2-2. Description of Reqd, Oper, and Slot Type fields

Field	Indicates
`Reqd`	Required operational state of the module, which can be `up`, `down`, or `maint`. This field reports the setting of the `reqd-state` parameter in the `slot-state` profile. See "Using slot-admin profiles" on page 2-8.
`Oper`	Current operational state of the slot, which can be one of the following values: ■ `UP`—Normal operational mode. ■ `DOWN`—Not in an operational mode. ■ `POST`—Module is running power-on self tests (POSTs). ■ `BOOT`—Control module has recognized the module and has begun to run the code in its boot ROM. Typically, the LOAD state quickly follows the BOOT state. ■ `LOAD`—Module is loading code as part of booting up. ■ `RESET`—Module is resetting. ■ `NONE`—Module has been removed, but its configuration remains in NVRAM. ■ `DIAG`—The slot is being controlled by a remote debugger or is trying to perform a core dump as the result of a fatal error.
`Slot Type`	Type of device installed in a slot, or the function defined by a virtual slot. For a list of all the devices, see the definition of the `slot-type` parameter in the *Stinger Reference*.

The system considers a module to be present if a `slot-type` profile exists for that type of module. If you remove a module, the system does not delete the `slot-type` profile for that module until you use the `slot -r` command or clear NVRAM. For more information, see "Removing a module and its configuration" on page 2-10.

Using the `rearslotshow` command

The `rearslotshow` command shows the status of all slots used for LPMs, path selector modules (PSMs), and copper loop test (CLT) modules. It also reports on the status of the midplane sparing bus. For details, see "Verifying port redundancy status" on page 4-12.

Viewing information about a particular module

You can obtain information about a particular module by entering the `show` command with the *`shelf-number`* and *`slot-number`* arguments or by displaying the `slot-info` profile.

Using the `show` command with the shelf and slot numbers

To use the `show` command for information about a particular module, add the shelf and slot numbers as arguments. For example:

```
admin> show 1 3
Controller { first-control-module } ( PRIMARY ):
                                Reqd  Oper   Slot Type
    { shelf-1 slot-3 0 }        UP    UP     al-dmtadsl-atm-card:
    { shelf-1 slot-3 1 }        DOWN       xdsl-12-line1
    { shelf-1 slot-3 2 }        DOWN       xdsl-12-line-2
    { shelf-1 slot-3 3 }        DOWN       xdsl-12-line-3
    { shelf-1 slot-3 4 }        DOWN       xdsl-12-line-4
    { shelf-1 slot-3 5 }        DOWN       xdsl-12-line-5
    { shelf-1 slot-3 6 }        DOWN       xdsl-12-line-6
    { shelf-1 slot-3 7 }        DOWN       xdsl-12-line-7
    { shelf-1 slot-3 8 }        DOWN       xdsl-12-line-8
    { shelf-1 slot-3 9 }        DOWN       xdsl-12-line-9
    { shelf-1 slot-3 10 }       DOWN       xdsl-12-line-10
    { shelf-1 slot-3 11 }       DOWN       xdsl-12-line-11
    { shelf-1 slot-3 12 }       DOWN       xdsl-12-line-12
```

The following sample command displays information about the trunk module installed in a Stinger MRT, which is identified as virtual slot 18 :

```
admin> show 1 18
      Shelf 1 ( standalone ):
                               Reqd Oper  Slot Type
 { shelf-1 trunk-module-2 0 } UP    UP   oc3-atm-trunk-daughter-card:
 { shelf-1 trunk-module-2 1 }       UP   atm-oc3-trunk-1
 { shelf-1 trunk-module-2 2 }       DOWN atm-oc3-trunk-2
```

Using the `slot-info` profile

The read-only `slot-info` profile stores information about each module that has successfully booted. This profile is not stored in NVRAM, so it does not persist across system resets or power cycles. The system creates a `slot-info` profile when you boot the module and deletes the profile when your remove or reboot the module. SNMP managers can read the `slot-info` profile.

The following sample commands display the contents of the `slot-info` profile for the module installed in slot 13:

```
admin> read slot-info {1 13 0}
SLOT-INFO/{ shelf-1 slot-13 0 } read

admin> list
[in SLOT-INFO/{ shelf-1 slot-13 0 }]
slot-address* = { shelf-1 slot-13 0 }
serial-number = 1018540161
software-version = 9.4-185.2
software-revision = 0
software-level = ""
hardware-level = 0
software-release = e0
```

For information about the parameters in the `slot-info` profiles, see the *Stinger Reference*.

Opening a session with a module

Each installed and operating LIM or T1 or E1 module on a Stinger FS, Stinger FS+, Stinger LS, or Stinger RT unit has its own processor and is running its own operating system. You can use the `open` command to connect to a module directly and run commands. On a Stinger MRT, you can open a session with virtual slot 1. (See "Understanding physical addressing on Stinger units" on page 2-1 for additional information.)

This type of connection is useful for performing debug operations, because when you issue a debug command from a module, the command operates only from the context of that module.

The syntax of the `open` command is as follows:

`open` *`shelf-number slot-number`*

Sample `open` commands

The `open` command creates an internal Telnet-like session with the module and displays a modified prompt indicating the slot and module you are managing.

Opening a session

The following command opens a session to the secondary control module in slot 9:

```
admin> open 1 9
shelf-router-1/9>
```

The following command opens a session to the LIM located in shelf 1, slot 4 of a Stinger FS, Stinger LS, or Stinger RT unit:

```
admin> open 1 4
dmtadsl-atm-1/4>
```

The following command opens a session with virtual slot 1 on a Stinger MRT:

```
admin> open 1 1
mrtdmt-1/1>
```

Ending a session

To exit the session with the module, enter `quit`, as in the following example:

```
dmtadsl-atm-1/4> quit
Terminated from far-end
```

Module-level commands

When you are connected to a module, only a subset of the Stinger commands are available. To list the commands available on the module, enter a question mark (`?`) or `help`, as in the following example:

```
dmtadsl-atm-1/4> ?
?                               ( user )
@fatalTest                      ( debug )
```

```
addrpool                        ( debug )
alErrs                          ( debug )
alPorts                         ( debug )
alRestart                       ( debug )
apctog                          ( debug )
arptable                        ( system )
atm1483State                    ( debug )
atmAdd                          ( debug )
atmApc                          ( debug )
atmARam                         ( debug )
atmAtab                         ( debug )
atmcacstat                      ( debug )
atmCacToggle                    ( debug )
atmcallif                       ( debug )
atmCktState                     ( debug )
atmCT                           ( debug )
atmDebug0                       ( debug )
atmDebug1                       ( debug )
atmDel                          ( debug )
atmDpRam                        ( debug )
[More? <ret>=next entry, <sp>=next page, <^C>=abort]
```

For information about module-level commands, see the *Stinger Reference*.

Changing a module's state

You can temporarily start or stop the operation of a module, put it in maintenance mode, or reset it by using the `slot` command or by setting the `reqd-state` parameter in the `slot-admin` profile. This feature is particularly useful while performing maintenance operations, when you might want to replace a failed module without deleting its configuration.

Using the `slot` command

The `slot` command allows you to control the state of an installed module. For the syntax of the `slot` command, see the *Stinger Reference*.

To temporarily stop the operation of a module, use the `slot` command with the `-d` option, and specify the module's shelf and slot number. For example:

```
admin> slot -d 1 3
slot 1/3 state change forced
```

When you stop a module's operation with the `slot` command, it remains disabled only until the next reboot, and retains its configuration.

To start the operation of a module, use the `slot` command with the `-u` option, and specify the module's shelf and slot number. For example:

```
admin> slot -u 1 3
slot 1/3 state change forced
```

Note You cannot change the state of a secondary control module by using the `slot -u` or `slot -d` commands.

To put a module in maintenance state, use the `-m` option. For example:

```
admin> slot -m 1 3
Slot 1/1, state change forced
warning: new state will remain until next explicit management action.
```

To reset a module, use the `slot` command with the `-b` option, and specify the shelf and slot number of the module you want to reset (bounce). For example:

```
admin> slot -b 1 3
slot 1/3 state change forced
```

Using `slot-admin` profiles

You can also change the state of a slot and its module using the `reqd-state` parameter in the `slot-admin` profile.

The following commands display the contents of the `slot-admin` profile for the module in slot 1. The parameter descriptions follow the profile listing.

```
admin> read slot-admin {1 1 0}
SLOT-STATE/{ shelf-1 slot-1 0 } read
```

```
admin> list
[in SLOT-ADMIN/{ shelf-1 slot-1 0 }]
slot-address* = { shelf-1 slot-1 0 }
reqd-state = reqd-state-up
```

Parameter	Setting
`slot-address`	Address of the slot.
`reqd-state`	Required operational state of the slot. If you change the value of this parameter to `nonoperational`, you temporarily disable a slot and its module. The change in status is complete when the setting of `current-state` parameter has changed to match the setting of the `reqd-state` parameter. The unit retains this setting only until you reset the system or remove power to the unit. At system startup, the system reinitializes the required state to match the actual state of the module. Specify one of the following values: ■ `reqd-state-down`—Requires the device to be in an inactive, nonoperational state. ■ `reqd-state-up`—Requires the device to be in a normal operating state. ■ `reqd-state-maint`—Requires the device be in a nonoperational maintenance state.

The following sample commands disable a slot:

```
admin> read slot-admin {1 3 0}
SLOT-STATE/{ shelf-1 slot-3 0 } read
```

```
admin> set reqd-state = reqd-state-down
```

```
admin> write
SLOT-STATE/{shelf-1 slot-3 0} written
```

The following commands return a slot to normal operating mode:

```
admin> set reqd-state = reqd-state-up
admin> write
SLOT-STATE/{ shelf-1 slot-3 0} written
```

Changing the state of a module's interface

You can change the state of an interface on a module by entering the `device` command or by setting the `reqd-state` parameter in the `device-state` profile. An interface is specified by its interface address, which consists of the shelf number (always 1), slot number, item number, and logical item number (if necessary) of the interface.

Using the `device` command

The `device` command initiates a state change to a specified interface on a module. You typically use this command to administratively disable or enable an interface.

For example, to administratively disable port 24 on a module in slot 3, use the `device` command with the `-d` option as follows:

```
admin> device -d {{1 3 24} 0}
device { { 1 3 24 } 0 } state change forced
```

To reenable the port, use the `device` command with the `-u` option as follows:

```
admin> device -u {{1 3 24} 0}
device { { 1 3 24 } 0 } state change forced
```

Using the `device-state` profile

Every host interface or network interface on a Stinger unit has a `device-state` profile, which stores the current state of an interface and allows you to change it.

The following commands display the `device` profile for port 24 in slot 3. The description of the parameters follow the profile listing.

```
admin> read device-state {{1 3 24} 0}
DEVICE-STATE/{ { shelf-1 slot-3 24 } 0 } read
admin> list
device-address* = { { shelf-1 slot-3 24 } 0 }
device-state = down-dev-state
up-status = idle-up-status
reqd-state = up-reqd-state
```

Parameter	Setting
`device-address`	Address of the device whose state is stored in this profile, defined by the address {{*shelf slot item*}} *logical item*}.
`device-state`	Current operational state of the interface, which can be `down-dev-state`, `up-dev-state`, or `none`. A status of `none` indicates that the interface does not exist on the unit.

Parameter	Setting
up-status	Status of an operational interface. This parameter is valid only if the device-state parameter is set to up-dev-state. An operational interface displays one of the the following values: ■ idle—Interface is not in use. ■ reserved—Interface is not used until all idle interfaces of the same type are in use. ■ assigned—Interface is in use.
reqd-state	Required operational state of the interface, which can be up-reqd-state or down-reqd-state. Changing this value initiates a state change for the interface. The change is complete when device-state parameter changes to match the reqd-state parameter. The Stinger unit retains this setting only until you reset or remove power to the unit. At system startup, the system reinitializes the required state to match the actual state of the interface.

The following commands disable port 24 on the device installed in slot 3:

```
admin> read device-state {{1 3 24} 0}
DEVICE-STATE/{ { shelf-1 slot-3 24 } 0 } read

admin> set reqd-state = down-reqd-state

admin> write
DEVICE-STATE/{ { shelf-1 slot-3 24 } 0 } written
```

Removing a module and its configuration

Stinger FS, Stinger FS+, Stinger LS, or Stinger RT modules are hot-swappable. When you remove a module, the system retains its configuration. This feature enables you to reinstall the module or install another of the same type in the same slot without reconfiguring the system or uploading a backup configuration. One side-effect of this feature is that when you remove a module, the NVRAM used to store configuration information is not cleared until you explicitly clear the configuration.

When you remove a module from a Stinger FS, Stinger FS+, Stinger LS, or Stinger RT unit, the show command reports a value of NONE. For example:

```
admin> show 1 4
Controller { first-control-module } ( PRIMARY ):
                                    Reqd  Oper   Slot Type
  { second-control-module }         UP    UP     ( SECONDARY )
  { shelf-1 slot-4 0 }              UP    NONE   stngr-32-idsl-card:
```

The status NONE indicates that the module was removed but its profiles have been saved. The Stinger unit saves the profile of modules that you have removed until you install a module of a different type in the same slot, or until you enter the slot -r command, as in the following example:

```
admin> slot -r 4
slot 1/4 removed
```

In either case, the system deletes all the old profiles associated with the slot. If you insert a different type of module, the system creates the appropriate new profiles.

Removing LIMs that use system-generated ATM addresses

In a Stinger unit enabled for Private Network-to-Network Interface (PNNI) protocol, the system generates a unique ATM address for each ATM interface via the `AtmInterfaceSoftPvcAddressTable`. These ATM addresses are used as the target address (`atmSoftPvccTargetAddress`) during the creation of a soft permanent virtual circuit (SPVC). The system generates the ATM addresses based on the LIM serial number, using the following formula:

```
SPVC address = pnni-node-prefix + LIM-serial-number + port-number
```

For details, see the *Stinger Private Network-to-Network Interface (PNNI) Supplement*.

Replacing a LIM and retaining the existing ATM addresses on the slot

If you replace a LIM and wish to retain the existing ATM addresses for the slot (whether the addresses were generated by the system or assigned explicitly), do *not* use the `slot -r` command. Simply remove the old LIM and insert the new LIM into the slot. The system recognizes the existing ATM addresses and does not generate new ones. An SPVC initiator switch can reestablish subscriber SPVCs, because the SPVC addresses have not changed.

Moving a LIM that uses system-generated ATM addresses

If you move a LIM to a slot that does not already have assigned ATM addresses, you must remove the configuration from the previous slot by using the `slot -r` command. Otherwise, when you insert the LIM into the new slot, the system generates new ATM addresses using the same formula based on the serial number of this LIM, which results in duplicate ATM addresses for the interfaces in two slots. If duplicate ATM addresses occur on multiple LIM interfaces, calls can be established only on one of the interfaces.

For example, suppose slot 4 contains a LIM that will be moved to slot *N*, and the LIM interfaces have system-generated ATM addresses based on the serial number of the LIM. Slot *N* has no addresses configured (for example, it has never been used or its configuration has been removed via `slot -r`). To move the LIM, you must follow this procedure:

1. Remove the LIM from slot 4.
2. Delete the configuration by using the `slot -r` command. For example:

   ```
   admin> slot -r 4
   ```
3. Insert the LIM into its new slot.
4. Save the new configuration using the `save` command.

After the move, slot 4 has no addresses configured. In slot *N*, the LIM interfaces have system-generated ATM addresses based on the serial number of the LIM. Saving the new configuration is recommended, to avoid the possibility of restoring old ATM address assignments.

Note If existing subscriber loops are connected to the LIM and you remove the configuration by using the `slot -r` command, when you insert a new LIM in that slot, the interfaces will have new ATM addresses. In that case, you must inform the SPVC

initiator switch of the new ATM addresses associated with the LIM to enable the switch to reestablish the subscriber SPVCs.

Loading specific module images

To access a specific control module, you can either Telnet to its configured IP address or connect by way of the control module's serial port. Once you have connected to the control module, you can use the `load-select` profile to load specific module images and images for newly released modules previously unknown to the system, from tar files. Using the `load` and `loadmate` commands, you can also load an extracted code image or transfer code images between control modules on redundant systems.

If the Stinger FS, Stinger FS+, Stinger LS, or Stinger RT unit contains two control modules, you must always load the same version of software to both control modules. Also, unless you specify otherwise, the system defaults to using the PCMCIA flash card in slot 1 of each control module.

Using the `load-select` profile

The `load-select` profile enables you to specify which module images to load to flash when you use a `load tar` command. For example:

```
admin> load tar network IPaddress stgrel.tar flash-card-2
```

After you reset a system, the system creates the `load-select` profile if it is not present. Each parameter in the `load-select` profile represents a supported module image and an intended load action for each module type, when the image is present in a tar file. It also contains an `unknown-cards` parameter, which represents new modules that were not supported in the previous TAOS release.

When loading the tar file, the system uses settings in the `load-select` profile to load only specific module images. For a listing of the parameters in the `load-select` profile, see the *Stinger Reference*. Each parameter in the profile represents a type of module installed on a Stinger FS, Stinger FS+, Stinger LS, Stinger RT unit, or port functions on a Stinger MRT.

The setting of the parameter for each module specifies the action that the system takes when the code image is present in a tar file. The `load-select` profile does not list the control module code, because that image is always loaded from the updated tar file. Specify one of the following settings:

- `auto` (the default)—Load images for modules that are installed in the Stinger unit and skip images for modules that are not installed.
- `load`—Load the image for the module, even if no module of that type is installed.
- `skip`—Skip the image for the module, even if a module of that type is installed.

The system determines a module to be present if a `slot-type` profile exists for that module type. It creates a `slot-type` profile when it first detects the presence of a module. If you remove that module, the system does not delete the `slot-type` profile for that module unless you use the `slot -r` command or clear NVRAM. To ensure that the system does not load unnecessary images, use `slot -r` to remove `slot-type` profiles for modules that are no longer installed in the system. For details, see "Removing a module and its configuration" on page 2-10.

.

Loading images for unknown modules

The `unknown-cards` parameter represents any module that was not supported in the previous release. If you install a new type of module into the Stinger unit before loading the tar file, the system loads all code images for all unknown modules, which can cause an overflow in the PCMCIA flash card or built-in flash memory. To prevent a flash overflow, use the following procedure:

1 Set the `unknown-cards` parameter in the `load-select` profile to `skip`.

```
admin> read load-select
LOAD-SELECT read

admin> set unknown-cards = skip

admin> write
LOAD-SELECT written
```

2 Save the current configuration to a TFTP server.

3 Load the new boot-loader from a TFTP server (or from the console). For example:

```
admin> load boot-cm network 10.10.10.10 stgcmb.bin
```

4 Load the tar file from a TFTP server (or from the console). For example:

```
admin> load tar network 10.10.10.10 stgrel.tar
```

5 Reset the system.

6 Install the new module.

7 Load the tar file again to delete the images that are not required. For example:

```
admin> load tar network 10.10.10.10 stgrel.tar
```

Loading an extracted code image

You can override the settings in the `load-select` profile by using the `load` command after you have extracted the tar file. For example, if the `sdsl-atm` parameter in the `load-select` profile is set to `skip`, you can load the image for that module by entering the following `load` command:

```
admin> load sdsl-atm network 10.10.10.10 stngrcsdsl.ffs
```

For additional information about the `load` command, see the *Stinger Reference*.

Using the `load configuration` command with an ATM VCC

If you are using an ATM virtual channel connection (VCC) as an inband management channel, be careful when downloading a configuration file with the `load configuration` command.

A `connection` profile and an associated `atm-qos` profile define each management channel. If the management channel's `connection` profile or `atm-qos` profile stored in the Stinger is different from the profile defined in the configuration file, the inband management channel might be disconnected during the load.

If the `connection` profile and associated `atm-qos` profile are different, proceed as follows to load the configuration successfully:

1 Delete the `connection` profile and associated `atm-qos` profile from the configuration file.

2 Load the modified configuration file.

3 Using the command-line interface, change the `connection` profile and associated `atm-qos` profile to match the profiles that were in the original configuration file.

If there is no difference between the profiles, then no special action is needed.

Recovering from a failed module installation

If you installed a new module in a Stinger FS, Stinger FS+, Stinger LS, or Stinger RT unit before upgrading the system software, and the module does not begin operating properly, you can attempt to recover using one of the following methods:

- Use the `nvram` command.
- Remove the module.

Using the `nvram` command

Caution Using the `nvram` command resets the entire system. You cannot perform this task remotely because the `nvram` command clears the Stinger unit configuration, including its IP address. Before performing this procedure, make sure that you have access to the Stinger unit's serial port.

To recover from a failed module installation using the `nvram` command, proceed as follows:

1 Save the current system configuration. For example:

```
admin> save network bonzo 971001
```

This command saves the configuration to a file named 971001 in the TFTP home directory on a host named `bonzo`.

2 Clear the system configuration and restart the Stinger unit by entering the `nvram` command:

```
admin> nvram
```

3 Restore the saved system configuration.

You can restore the configuration through the serial port, or you can reassign an IP address and default gateway through the serial port, then use the `load` command to load the rest of the configuration, as in the following example:

```
admin> load config network bonzo 971001
```

This command restores the configuration from a file named 971001 in the TFTP home directory on a host named `bonzo`.

For a complete description of saving and restoring configurations, see Chapter 1, "Administering a Stinger System"

Removing the module

To recover from a failed module installation by removing the module:

1 Save the current configuration of any profiles on the module. For example:

```
admin> save network bonzo 971001 ds3-atm
```

This command saves the configuration of all DS3-ATM profiles for this trunk module to a file named 971001 in the TFTP home directory on a host named `bonzo`.

2 Stop the module's operation, as in the following example:

```
admin> slot -d 1 1
```

This command disables the module in shelf 1, slot 1.

3 Remove the module profile:

```
admin> slot -r 1 1
```

4 Reenable the module:

```
admin> slot -u 1 1
```

5 Restore the configuration of any profiles on the module. For the DS3-ATM trunk module in this example, you enter the following command:

```
admin> load config network bonzo 971001
```

This command restores the configuration from a file named 971001 in the TFTP home directory on a host named `bonzo`.

Monitoring the Stinger Unit 3

A Stinger unit includes mechanisms for maintaining the integrity of ATM cell-processing application-specific integrated circuits (ASICs) for control modules and line-interface modules (LIMs).

The Stinger unit monitors itself continuously and generates error and event messages related to its operations. It also monitors itself for alarm events, such as failures and state changes. For information about remote monitoring using SNMP, see "Administering the SNMP Agent" on page 9-1.

Maintaining ASIC Integrity

Because the ATM cell-processing application-specific integrated circuits (ASICs) are so central to the unit's performance, error detection and correction mechanisms are supported for both the control module and LIM ASICs.

The default `system-integrity` profile configuration for control modules enables continuous background testing of the control module ASIC. Lucent Technologies recommends that you do not disable this default.

The default `system-integrity` configuration for LIM testing is a periodic integrity test for those LIMs that support it, and a periodic reset for earlier LIMs that are not equipped for integrity testing (STGR-LIM-AD-12 and STGR-LIM-SH-48). You can configure the control module to perform LIM integrity testing centrally, as described in "Enabling centralized integrity checks" on page 3-4.

Checking the defaults for control module self-tests

If a problem occurs in the control module's ATM ASIC, the unit might stop switching data traffic. To prevent this possibility, by default, the system performs background integrity tests of the control module ASIC at a specified interval of 100 milliseconds. The system keeps track of the past 20 integrity tests, and verifies after each test how many failures have occurred in the previous 20 tests. If this failure rate is higher than the configured correction factor, the control module performs a correction by resetting its ASIC.

Following are the `integrity-config` subprofile settings, shown with default values for a control module in slot 8. With the default configuration, continuous checking is enabled, and Lucent Technologies recommends that you keep this default.

```
[in SYSTEM-INTEGRITY:integrity-config[8]]
enable-continuous-detection = yes
detection-interval = 100
only-one-correction = yes
correction-factor = 5
auto-correction-enable = yes
interval-auto-correction = 600000
```

Parameter	Setting
`enable-continuous-detection`	Enable/disable detection and correction in continuous mode. The default of `yes` is recommended for the control modules.
`detection-interval`	Detection interval in milliseconds. When continuous detection is enabled, the control module performs integrity tests at defined intervals. Valid values are from 0 to 65535. **Note** The default value of 100ms is recommended for control modules.
`only-one-correction`	Enable/disable multiple corrections in a row. The default `yes` value causes the system to apply the ASIC correction only once. Only one correction is recommended.
`correction-factor`	Number of problems that must be detected in the previous 20 integrity tests to cause a correction. With the default value of 5, a correction results if the system detects five problems in its history of 20 previous tests. Valid values are from 1 to 20.
`auto-correction-enable`	*Does not apply to control modules.*
`interval-auto-correction`	*Does not apply to control modules.*

LIM automatic correction settings

By default, detection and correction of the LIM ASICs are performed every few hours or at a specified interval. For earlier LIMs that are not equipped for integrity testing (STGR-LIM-AD-12 and STGR-LIM-SH-48), the ASIC is simply reset automatically. For recent LIMs that can perform integrity testing, instead of an automatic correction, an integrity test is performed every few hours and the ASIC is corrected only if a problem is detected.

Following are the `integrity-config` settings for LIM ASIC integrity testing, shown with default values for a LIM in slot 1:

```
[in SYSTEM-INTEGRITY:integrity-config[1]]
```

```
enable-continuous-detection = no
detection-interval = 100
only-one-correction = yes
correction-factor = 5
auto-correction-enable = yes
interval-auto-correction = 600000
```

Parameter	Setting
`enable-continuous-detection`	Enable/disable detection and correction in continuous mode. The default value is `no` for LIM slots, which allows sufficient correction for most LIMs while conserving system resources.
`detection-interval`	Detection interval in milliseconds. The default value is 100ms. Valid values are from 0 to 65535. When continuous detection is enabled, the LIM performs integrity tests at the defined interval.
`only-one-correction`	Enable/disable multiple corrections in a row. If the unit is configured to perform only one correction, after resetting the ASIC, the control module erases the previous 20 tests and begins again. This mechanism prevents multiple resets if the past few tests have failed continuously, and is the recommended setting.
`correction-factor`	Number of problems that must be detected in the previous 20 integrity tests to cause a correction. Valid values are from 1 to 20. The default is 5.
`auto-correction-enable`	Enable/disable automatic correction for the LIM. With the default `yes` value, the LIM performs an integrity test (for LIMs equipped for integrity testing) or performs a correction at the interval specified by the `interval-auto-corection` parameter. If this parameter is set to `no`, the LIM performs these actions every 2 to 3 hours.
`interval-auto-correction`	Number of milliseconds between LIM automatic correction actions. The default is 600000ms (10 minutes). Valid values are from 0 to 2147483647.

For example, the following commands verify that a 12-port SDSL LIM resides in slot 14 and change the automatic correction interval for that LIM to 1 hour:

```
admin> show
Controller { first-control-module } ( PRIMARY ):
                              Reqd  Oper   Slot Type
 { shelf-1 slot-3 0 }         UP    UP     dadsl-atm-24-card
 { shelf-1 slot-14 0 }        UP    UP     sdsl-atm-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> read system-integrity
SYSTEM-INTEGRITY read
```

```
admin> set integrity-config 14 interval-auto-correction = 3600000
admin> write
SYSTEM-INTEGRITY written
```

Enabling centralized integrity checks

In addition to the periodic automatic correction performed by the LIMs, you can enable centralized detection, which causes the control module to perform integrity tests on every LIM in the unit that is equipped for ASIC testing. If a LIM requires correction, the control module sends a message causing the LIM to reset its ASIC. If the LIM problem is not corrected within 5 minutes, the control module resets the LIM ASIC again and also resets its own ASIC. Resetting both the control module and LIM ASICs at the same time clears most problems.

Note By default, all LIMs are corrected every few hours, which is typically sufficient for most LIMs.

Following are the relevant parameters, shown with default values:

```
[in SYSTEM-INTEGRITY]
enable-centralized-detection = no
ratio-centralized-detection = 5
```

Parameter	Setting
`enable-centralized-detection`	Enable/disable centralized error detection. This option is disabled by default. If the parameter is set to `yes`, the control module is required to perform LIM testing using its own failure ratio and correction setting. If a LIM requires a reset of the ASIC, the control module sends a message to the LIM to initiate the reset. If the reset does not correct the detected problem within 5 minutes, the control module initiates a second LIM reset and simultaneously resets its own ASIC.
`ratio-centralized-detection`	If centralized detection is enabled, this parameter specifies the ratio of problem detection between the control module and all other modules. For example, if the ratio is 5, the control module performs five self-tests before triggering centralized LIM tests. Values can be from 0 to 65535. The default is 5.

For example, the following commands enable centralized detection and specify a ratio of 100. Because the control module self-tests are performed every 100ms by default, this ratio causes the control module to perform LIM testing every 10 seconds.

```
admin> read system-integrity
SYSTEM-INTEGRITY read
admin> set enable-centralized-detection = yes
admin> set ratio-centralized-detection = 100
admin> write
SYSTEM-INTEGRITY written
```

Defining alarms

You can configure the Stinger unit to monitor itself for certain alarm conditions or events and specify an action that it takes when it detects the alarm condition. You use the `alarm` profile to configure the Stinger unit's status lights and alarm relays to respond to alarm conditions as follows:

- Configure status lights to illuminate in response to alarm conditions.
- Configure alarm relays to open or close for a specified number of seconds in response to alarm conditions.
- Configure a default `alarm` profile for the entire system.
- View `alarm` profiles.
- View outstanding alarms.

You can use a Stinger FS, Stinger FS+, Stinger LS, or Stinger RT unit installed with revision 2 control modules A, B, A-J, or C to monitor the status of up to seven devices. A Stinger MRT unit can monitor up to four remote devices. For additional information, see the *Getting Started Guide* for your unit at `http://www.lucentdocs.com/ins.`

Overview of `alarm` profile settings

You can define an alarm profile for every event that you would like to monitor. Following is a listing of the `alarm` profile contents, shown with default settings. For additional information about these parameters, see the *Stinger Reference*.

```
[in ALARM/"" (new)]
name* = ""
enabled = no
event = line-state-change
physical-address = { any-shelf any-slot 0 }
action = { off off off 0 off 0 }

[in ALARM/"":action (new)]
alarm-led-minor = off
alarm-led-major = off
alarm-relay-minor = off
alarm-relay-minor-duration = 0
alarm-relay-major = off
alarm-relay-major-duration = 0
```

Parameter	Setting
`name`	User-defined name of the `alarm` profile.
`enabled`	Enable/disable the `alarm` profile. Specify `yes` to enable or `no` (the default) to disable this profile.
`event`	Event that triggers an alarm, which results in action specified by the settings in the `action` subprofile. Specify one of the following events: ■ `power-failure`—Redundant power supply failure. ■ `fan-failure`—Redundant fan failure

Parameter	Setting
	■ `line-state-change` (the default)—Change in the state of a line. ■ `slot-state-change`—Change in the state of a slot. ■ `input-relay-closed`— Input relay monitoring circuit is closed. The alarm is cleared whenever the circuit is reopened. ■ `input-relay-open`—Relay monitoring circuit is open. The alarm is cleared whenever the circuit is closed. ■ `primary-switchover`—Change in the primary control module. ■ `secondary-controller-state-change`—Change in the state of the secondary control module. ■ `low-temperature-trigger`—Low-temperature threshold is crossed. ■ `high-temperature-trigger`—High-temperature threshold is crossed.
`physical-address`	Physical address of the entity that is being monitored by this alarm, as defined by its slot number or item-number. The `physical-address` parameter applies only to `line-state-change` or `slot-state-change` events.
`action`	Subprofile that specifies the actions that the Stinger unit performs when it detects the event specified by the `event` parameter. Set the following parameters.
`action: alarm-led-major`	Enable/disable the MAJOR alarm status light to illuminate when the system detects the specified event. Set to `on` to enable. The default setting is `off`.
`action: alarm-led-minor`	Enable/disable the MINOR alarm status light to illuminate when the system detects the specified event. The default setting is `off`.
`action: alarm-relay-major`	Enable/disable the relay for the MAJOR alarm relay circuit to close or open when the system detects the specified event. If set to `on`, the major alarm relay closes (if it is normally open) or opens (if it is normally closed) when the system detects the specified event. The default setting is `off`.
`action: alarm-relay-major-duration`	Number of seconds that the Stinger unit leaves `alarm-relay-major` in the position specified in the `alarm-relay-major` action. The default setting of zero (`0`) directs the system to leave the alarm set indefinitely.
`action: alarm-relay-minor`	Enable/disable the relay for the MINOR alarm relay circuit to close or open when the system detects the specified event. If set to `on`, the minor alarm relay closes (if it is normally open) or opens (if it is normally closed) when the system detects the specified event. The default setting is `off`.

Parameter	Setting
alarm-relay-minor-duration	Number of seconds that the Stinger unit leaves alarm-relay-minor in the position specified in the alarm-relay-minor action. The default value 0 (zero) directs the Stinger unit to leave the alarm set indefinitely.

Sample `alarm` profile configuration

The following example configures a Stinger unit to close the relay for the MAJOR alarm for 10 minutes when the redundant power supply fails:

```
admin> read alarm alarm-1
ALARM/alarm-1 read
admin> set enable = yes
admin> set event = power-fail
admin> set physical-address = {0 0 0}
admin> set action alarm-led-major = on
admin> set action alarm-led-minor = off
admin> set action alarm-relay-major = on
admin> set action alarm-relay-major-duration = 600
admin> set action alarm-relay-minor = off
admin> set action alarm-relay-minor-duration = 0
admin> write
ALARM/alarm-1 written
```

By setting the physical-address parameter in an alarm profile to 0 0 0 (any shelf, any slot, any item), you can apply an alarm profile to the entire Stinger unit.

Working with alarms

You can use the alarm command or the alarm-stat profile to list alarms and their status, or acknowledge and clear them.

Listing alarms using the `alarm` command

To list the alarms that are enabled for the entire Stinger unit, use the alarm -l command as in the following example:

```
admin> alarm -l
Name         Address            Event
lalit        {  0  0  0 }       Input Relay Open
satish       {  0  0  0 }       Primary Switchover
success      {  1  1  0 }       Slot State Change
test1        {  1  2  0 }       Line State Change
test2        {  0  0  0 }       Fan Failure
```

To list the alarms that are enabled for a specific physical address, use the alarm -l command as in the following example:

```
admin> alarm -l 1 0 0
Name         Address            Event
```

```
success      {  1  1  0 }       Slot State Change
test1        {  1  2  0 }       Line State Change
```

To specify all the Stinger unit's alarms, enter the `alarm` command with the `-s` option:

```
admin> alarm -s
         Type            Address   State
 Secondary CM Down      -- -- --   Active
 Line Down            {  1 17  1 } Active
 Line Down            {  1 17  2 } Active
 Line Down            {  1 18  1 } Active
 Line Down            {  1 18  2 } Active
```

To display only the alarms for a particular module, specify the shelf (always 1) and slot number, as shown in the following example:

```
admin> alarm -s 1 17
   Type                 Address   State
 Line Down            {  1 17  1 } Active
 Line Down            {  1 17  2 } Active
```

To display only the alarms for a particular line, specify the shelf, slot, and item number, as shown in the following example:

```
admin> alarm -s 1 17 1
   Type                 Address   State
 Line Down            {  1 17  1 } Active
```

Using the `alarm-stat` profile

The `alarm-stat` profile enables you to monitor and change the status of alarms. The system creates an `alarm-stat` profile whenever an alarm condition exists and deletes them when the alarm condition no longer exists or is cleared by the `alarm` command. The `alarm-stat` profile listing displays the physical address of the device in an alarm state, as well as the type of alarm condition.

In the following example, the first two lines in trunk module 1 are in a line-state change alarm condition:

```
admin> dir alarm-stat
0  06/20/1999 17:23:20  { { shelf-1 trunk-module-1 1 } line-state-change }
0  06/20/1999 17:23:49  { { shelf-1 trunk-module-1 2 } line-state-change }
```

The following commands list the contents of the `alarm-stat` profile. The parameter descriptions follow the profile listing.

```
admin> read alarm-stat { { shelf-1 trunk-module-1 1 } line-state-change }
ALARM-STAT/{ { shelf-1 trunk-module-1 1 } line-state-change+ read

admin> list
[in ALARM-STAT/{ { shelf-1 trunk-module-1 1 } line-state-change+]
alarm-id* = { { shelf-1 trunk-module-1 1 } line-state-change }
alarm-state = alarm-active
```

Parameter	Setting
`alarm-id`	Physical address of the device that has the alarm condition and the alarm event.

Parameter	Setting
alarm-state	State of the alarm. Following are the valid values: ■ alarm-active—The alarm is active, and appropriate action has been taken (setting status lights or closing relays). ■ alarm-acknowledged—The alarm has been acknowledged by the user.

Acknowledging alarms

To acknowledge alarms, use the alarm command with the -a option. The following example shows how to acknowledge the alarms for line 1 in slot 17:

```
admin> alarm -a 1 17 1
```

When you use the alarm -s command, the output shows that the alarm for the first line in slot 17 has been acknowledged:

```
admin> alarm -s
     Type              Address    State
 Secondary CM Down     -- -- --   Active
 Line Down            {  1 17  1 } Acknowledged
 Line Down            {  1 17  2 } Active
 Line Down            {  1 18  1 } Active
 Line Down            {  1 18  2 } Active
```

Clearing alarms

You can use the alarm command or the alarm-state parameter to clear an alarm.

To clear an alarm using the alarm command, use the -c option. The following example shows how to clear the alarms for line 1 slot 18:

```
admin> alarm -c 1 18 1
```

Using the -s option shows that the alarm for the first line in slot 18 has been cleared and thus no longer appears on the list of alarms:

```
admin> alarm -s
     Type              Address     State
 Secondary CM Down      -- -- --   Active
 Line Down            {  1 17  1 } Acknowledged
 Line Down            {  1 17  2 } Active
 Line Down            {  1 18  2 } Active
```

Configuring alarm support for alarm MIB

Stinger units support alarm management information bases (MIBs) as described in draft-ietf-disman-alarm-mib-04.txt. The MIBs provide the following information:

- All possible alarms in the system
- Currently active alarms in the system
- Cleared alarms in the system

To set the maximum number of alarms in alarmClearTable, set the alarm-clear-table-limit parameter in the snmp profile. See "alarm-clear-table-

limit" on page 9-3. For example, the following sample commands specify that up to 150 alarms can be stored in `alarmClear` Table:

```
admin> read snmp
SNMP read
admin> set alarm-clear-table-limit = 150
admin> write
SNMP written
```

Clearing alarms from `alarmActiveTable` and `alarmClearedTable`

To clear the alarms in `alarmActiveTable` and `alarmClearTable`, disable the associated `trap` profile by setting the `active-enabled` parameter in the `trap` profile to `no`. If the `trap` profile is disabled, the alarm model table reports `RowStatus` as `NOT_IN_SERVICE`. For more information about enabling traps and working with a `trap` profile, see the a"Defining alarms" on page 3-5.

Deleting an alarm model table

To delete an alarm model table, delete the corresponding `trap` profile.

Turning off an alarm status light

The `ledoff` command turns off an alarm status light. To turn off a MAJOR alarm status light, use the `ledoff` command with the `major` option. To turn of a MINOR alarm status light, use the `ledoff` command with the `minor` option. For example:

```
admin> ledoff major
```

Closing a relay

The `relayoff` command closes or opens a relay circuit that has been activated by an alarm. To turn off a MAJOR relay circuit, use the `relayoff major` command. To turn of a MINOR relay, use the `relayoff` command with the `minor` option. For example:

```
admin> relayoff major
```

Configuring alarms for ADSL threshold values

Stinger units can generate traps for alarms when certain ADSL line conditions reach specified threshold values. To enable the supported threshold traps in the ADSL MIB, perform the following tasks:

- Specify the `dsl-threshold` profile to be used for a line by setting the `thresh-profile` parameter in the line's `al-dmt` profile.
- Configure the parameters in the `dsl-threshold` profile that specify threshold values for SNMP alarms on ADSL lines.

The index of the `dsl-threshold` profile is the name of the profile. Each `dsl-threshold` profile is not tied to a particular line, but is linked instead by the `thresh-profile` parameter of an `al-dmt` profile for that line. During startup, the system creates a default `dsl-threshold` profile named `default` and also sets the `thresh-profile` parameter in each `al-dmt` profile to `default`, creating the link between the profiles.

In the SNMP interface, `default` is displayed as `DEFVAL`, as defined by RFC 2662.

Specifying the dsl-threshold profile

The thresh-profile parameter in the al-dmt profile specifies the dsl-threshold profile to use for an ADSL line. The thresh-profile parameter is shown below with its default setting, default:

```
[in AL-DMT/{ shelf-1 slot-1 22 }]
thresh-profile = default
```

Parameter	Setting
thresh-profile	Name of the dsl-threshold profile that sets threshold traps for this ADSL line. By default, this parameter is set to default, which is the name of the default dsl-threshold profile.

Overview of the dsl-threshold profile settings

Following are the parameters for the dsl-threshold profile with default settings:

```
[in DSL-THRESHOLD/default (new)]
name* = default
enabled = no
atuc-15min-lofs = 0
atuc-15min-loss = 0
atuc-15min-lols = 0
atuc-15min-lprs = 0
atuc-15min-ess = 0
atuc-fast-rate-up = 0
atuc-interleave-rate-up = 0
atuc-fast-rate-down = 0
atuc-interleave-rate-down = 0
atuc-init-failure-trap = disable
```

Parameter	Setting
name	Name of the dsl-threshold profile. To set the threshold times for an ADSL line, specify the name of a dsl-threshold profile in the thresh-profile parameter of the al-dmt profile. Enter a text string of up to 23 characters.
enabled	Enable/disable this profile. Specify yes to enable the profile. This parameter must be set to yes if any of the following settings are to apply.
atuc-15min-lofs	Number of loss-of-frame seconds encountered by a DSL interface within any given 15-minute performance data collection period, which causes the SNMP agent to send a trap. One trap is sent per interval, per interface. A value of 0 disables the trap. Enter a value from 0 through 900.
atuc-15min-loss	Number of loss-of-signal-seconds encountered by a DSL interface within any given 15-minute performance data collection period, which causes the SNMP agent to send a trap. One trap is sent per interval, per interface. A value of 0 disables the trap. Enter a value from 0 through 900.

Parameter	Setting
atuc-15min-lols	Number of loss-of-link seconds encountered by a DSL interface within any given 15-minute performance data collection period, which causes the SNMP agent to send a trap. One trap is sent per interval per interface. A value of 0 disables the trap. Enter a value from 0 through 900.
atuc-15min-lprs	Number of loss-of-power seconds encountered by a DSL interface within any given 15-minute performance data collection period, which causes the SNMP agent to send a trap. One trap is sent per interval per interface. A value of 0 disables the trap. Enter a value from 0 through 900.
atuc-15min-ess	Number of errored seconds encountered by a DSL interface within any given 15-minute performance data collection period, which causes the SNMP agent to send a trap. One trap is sent per interval per interface. A value of 0 disables the trap. Enter a value from 0 through 900.
atuc-fast-rate-up	Change in rate of a fast channel causing a trap to be sent. A trap is produced when ChanCurrTxRate is greater than or equal to the value of this parameter added to the ChanPrevTxRate. Enter a value from 0 through 2147483647. A value of 0 disables the trap.
atuc-interleave-rate-up	Change in rate of an interleaved channel causing a trap to be sent. A trap is produced when ChanCurrTxRate is greater than or equal to the value of this parameter added to the ChanPrevTxRate. Enter a value from 0 through 2147483647. A value of 0 disables the trap.
atuc-fast-rate-down	Change in rate of a fast channel causing a trap to be sent. A trap is produced when ChanCurrTxRate is less than or equal to the value of this parameter added to the ChanPrevTxRate. Enter a value from 0 through 2147483647. A value of 0 disables the trap.
atuc-interleave-rate-down	Change in rate of an interleaved channel causing a trap to be sent. A trap is produced when ChanCurrTxRate is less than or equal to the value of this parameter added to the ChanPrevTxRate. Enter a value from 0 through 2147483647. A value of 0 disables the trap.
atuc-init-failure-trap	Enable/disable InitFailureTrap.

Configuring system logging and Syslog services

The Stinger unit generates error and event messages related to its operations. You can use the log profile to perform the following tasks:

- Configure how the system handles log messages that are displayed on a status window. (See also, "Setting log levels for each login" on page 1-15.)
- Enable and configure the system to save log messages to the Syslog server.

Overview of log profile parameters

The following commands display the contents of the log profile and auxiliary-syslog subprofile, shown with default settings. Parameter descriptions follow the profile listing.

```
admin> read log
LOG read

admin> list

[in LOG]
save-level = info
save-number = 100
software-debug = no
call-info = none
syslog-enabled = no
host = 0.0.0.0
port = 514
facility = local0
syslog-format = tnt
log-call-progress = no
log-software-version = no
syslog-level = info
auxiliary-syslog = [ { no info 0.0.0.0 514 local0 } { no info 0.0.0.0 514
local

admin> list auxiliary-syslog
[in LOG:auxiliary-syslog]
auxiliary-syslog[1] = { no info 0.0.0.0 514 local0 }
auxiliary-syslog[2] = { no info 0.0.0.0 514 local0 }

admin> list 1
[in LOG:auxiliary-syslog[1]]
syslog-enabled = no
syslog-level = info
host = 0.0.0.0
port = 514
facility = local0
```

Parameter	Setting
save-number	Maximum number of log messages that the Stinger unit saves for display in the status windows.

Parameter	Setting
save-level	Lowest level of log messages that the Stinger unit displays in the log status window. The unit logs all messages that are at the specified level or higher. For example, if alert is specified, all messages at the alert and emergency levels are logged. Specify one of the following settings: ■ none (the default)—Displays no log messages. ■ emergency—Announces error conditions that are likely to prevent normal operation. ■ alert—Announces error conditions that do not prevent normal operation. ■ critical—Announces interface failures and security errors. ■ error—Announces error events. ■ warning—Displays unusual events that do not affect normal operation. ■ notice—Displays operational events of interest. ■ info—Displays state and status changes. ■ debug—Displays helpful debug information. The save-level parameter does not control the level of syslog records sent to a syslog server.
call-info	*Does not apply to the Stinger unit.*
syslog-enabled	Enable/disable the forwarding of log messages to a syslog server.
host	Domain Name System (DNS) hostname or address of a syslog host for the first data stream. In the auxiliary-syslog [1] subprofile, the host value specifies the host to which the unit sends syslog messages for the second data stream. In the auxiliary-syslog [1] subprofile, the host value specifies the host to which the unit sends syslog messages for the third data stream.
port	Destination port of the syslog host that receives the first data stream. In the auxiliary-syslog [1] subprofile, the port value specifies the destination port of the syslog host that receives the second data stream. In the auxiliary-syslog [1] subprofile, the port value specifies the destination port of the syslog host that receives the third data stream.

Parameter	Setting
facility	Syslog daemon facility code for messages logged from the Stinger unit. For detailed information, see the syslog.conf manual page entry on the UNIX syslog server. Specify one of the following settings: ■ local0 (the default) ■ local1 ■ local2 ■ local3 ■ local4 ■ local5 ■ local6 ■ local7 In the auxiliary-syslog [1] subprofile, the facility value applies to the second data stream. In the auxiliary-syslog [2] subprofile, the facility value applies to the third data stream. The settings in each auxiliary-syslog subprofile affect an individual syslog stream, and override the setting in the log profile.
log-call-progress	Enable/disable the unit to log incoming call-progress messages. Specify one of the following values: ■ yes—The unit logs incoming call-progress messages.s ■ no (the default)—The unit discards incoming call-progress messages.
log-software-version	Enable/disable the hourly log message reporting of the current software version to the syslog host. Specify yes to enable hourly log messages reporting the current software version or no (the default) to disable it. If debug permission is enabled, the messages are displayed on the screen (as well as sent to the syslog host).

Parameter	Setting
syslog-level	Lowest level of log messages that the Stinger unit sends to the syslog server. All levels above the level you indicate are included in your syslog messages. For example, if alert is specified, messages at the emergency and alert levels are included. Values are the same as those for save-level on page 3-14. By default, syslog records with a level of debug are filtered out, and records with a level of info or above are transmitted to the syslog server. The syslog-level value in the log profile affects all data streams. The syslog-level value in each auxiliary syslog subprofile affects the individual data stream directed to the device specified by the host value, and overrides the value in the log profile.
auxiliary-syslog [1]	Subprofile that specifies the settings for the syslog server for the second data stream.
auxiliary-syslog [2]	Subprofile that specifies the settings for the syslog server for the third data stream.

Configuring system logging

The Stinger unit records system events in its status window event log. (For additional information, see "Log message information" on page 1-39.)

The save-level parameter specifies the lowest level of message to be saved for status display. The lowest possible level is none (the default). The highest level is debug. For a list of the log message levels, see the description of save-level on page 3-14.

The save-number parameter specifies the number of messages to be saved in the status display. The default is 100.

The following commands configure the Stinger unit to save 200 messages in the event log and to display emergency type messages on the status display:

```
admin> read log
LOG read

admin> set save-level = emergency

admin> set save-number = 200

admin> write
LOG written
```

Configuring the Stinger unit Syslog facility

By configuring the Stinger unit to report events to a syslog host on the local IP network, you can maintain a permanent log of events and send Call Detail Reporting (CDR) reports to a host that can record and process them.

The host running a syslog daemon is typically a UNIX host, but it can also be a Microsoft Windows system. If the log host is not on the same subnet as the Stinger

unit, the unit must have a route to that host, either via RIP or a static route. (For information about `syslog` messages, see "Syslog messages" on page B-7.)

Note Do not configure the Stinger to send reports to a `syslog` host that can be reached only by a dial-up connection. Doing so causes the Stinger unit to dial the log host for every logged action, including hangups.

Enabling the Syslog facility on the Stinger unit

The following sample commands enable `syslog` reporting

```
admin> read log
LOG read
admin> set syslog-enabled = yes
```

Configuring Syslog streams

The stream of records sent by the Stinger unit to a `syslog` server is called a `syslog` *stream*. The Stinger unit supports up to three `syslog` servers and define an independent `syslog` stream for each server.

For example, you can define a `syslog` stream to transfer all records, another stream to transfer records with a severity level of `warning` or above, and a third stream to transfer records with a severity level of `emergency`.

The `syslog-format` parameter controls the format of all `syslog` streams. The parameters in the `log` profile and two auxiliary `syslog` subprofiles configure the `syslog` streams as follows:

- The `syslog-level`, `host`, `port`, and `facility` settings in the `log` profile affect the first data stream.
- The `syslog-level`, `host`, `port`, and `facility` settings in the `auxiliary-syslog [1]` subprofile affect the second data stream and override the settings in the `log` profile.
- The `syslog-level`, `host`, `port`, and `facility` settings in the `auxiliary-syslog [2]` subprofile affect the the third data stream and override the settings in the `log` profile.

The following sample commands define the first data stream and direct the Stinger unit to send end-of-call `syslog` messages to the host 10.2.3.4 on port 588:

```
admin> read log
LOG read
admin> set host = 10.2.3.4
admin> set port = 588
admin> set facility = local0
admin> write
LOG written
```

Note After setting a log facility number, configure the `syslog` daemon to write all messages containing that facility number to a particular log file. This file is the Stinger log file.

Specifying a session ID base

The `sessionid-base` parameter in the `system` profile specifies the base number to use for generating a unique ID for each session. The system uses this value to identify the session to SNMP, RADIUS, or other external entities If this parameter is set to zero, the Stinger unit sets the initial base for session IDs to the absolute clock. For details about this parameter, see the *Stinger Reference*.

Configuring the Syslog daemon

To configure the `syslog` daemon to interact with a Stinger system, you must modify the file `/etc/syslog.conf` on the host. This file specifies the action that the daemon performs when it receives messages from a particular log facility number (which represents the Stinger).

For example, if you set the `log` parameter `facility` to `local5` in the Stinger unit, and want to log its messages in `/var/log/Stinger01`, add the following line to `/etc/syslog.conf`:

```
local5.info<tab>/var/log/Stinger01
```

Note The `syslog` daemon must reread `/etc/syslog.conf` after it has been changed.

Configuring call logging

The call-logging protocol supports real-time surveillance of Stinger units using the Navis™ family of network management products. If configured, it allows NavisAccess™ 5.1 and later releases to monitor, report, and send alarms on various performance and failure information for the Stinger unit. For additional information, go to `http://www.lucent.com/products/` and search on `NavisAccess`.

Overview of call logging

The main purpose of Stinger call logging is to provide details about physical-layer line statistics to a management station for all active DSL OC3, DS3, and E3 trunk lines in a Stinger unit.

The Stinger unit uses a method called *streaming* to periodically collect call-logging data and send it to call-logging servers in an evenly distributed manner.

Once you have configured call logging, the Stinger unit sends Start Session, Stop Session, and Streaming packets to a call-logging server. A call-logging server is a local host that is configured properly to communicate with the Stinger, such as a host running NavisAccess™ software.

DSL statistics are generated on the DSL drivers of Stinger LIMs and trunk modules. These statistics are propagated to the management station by means of the call-logging protocol. The call-logging packets on the Stinger unit deliver ADSL, SDSL, HDSL, SHDSL, IDSL, OC3, E3, or DS3 statistics about the physical layer.

Note Call logging for the Stinger unit is supported by NavisAccess™ 5.1 or later releases.

Enabling call logging

To enable Stinger call logging to a call-logging server on the local network, proceed as in the following example:

1 Read in the `call-logging` profile:

```
admin> read call-logging
CALL-LOGGING read
```

2 Enable call logging:

```
admin> set call-log-enable = yes
```

3 Specify the IP address of a call-logging host:

```
admin> set call-log-host-1 = 10.2.3.4
```

4 Specify the number of seconds that the Stinger unit waits for a response to a call-logging request:

```
admin> set call-log-timeout = 10
```

5 Specify that the unit can send a stop packet without a username:

```
admin> set call-log-stop-only = yes
```

6 Specify a retry limit in seconds for call-logging requests to the host:

```
admin> set call-log-limit-retry = 3
```

7 Write the profile to save the changes:

```
admin> write
CALL-LOGGING written
```

Monitoring Interfaces on LIMs and Trunk Modules

4

TAOS includes profiles and commands that enable you to gather data specific to each interface or port on a Stinger line-interface module (LIM) or trunk module and each line interface on a Stinger MRT chassis. In this guide, *Stinger MRT* refers to the Stinger MRT 23 and Stinger MRT 19 chassis.

For information about how to monitor the ATM interfaces of a Stinger unit, see "Monitoring ATM and PNNI" on page 7-1.

For information about Ethernet and IP interfaces on Stinger control modules or a Stinger MRT chassis, see the *Getting Started Guide* for your unit. For information about Ethernet and IP interfaces on the Stinger T1000 module, see the *Stinger T1000 Module Routing and Tunneling Supplement*. For information about Ethernet and IP interface on the IP2000 control module, see the *Stinger IP2000 Configuration Guide*.

Summary of profiles and commands for monitoring interfaces

Table 4-1 summarizes the status profiles and commands that you use to monitor the physical interfaces of Stinger LIMs, trunks, and interfaces on the Stinger MRT chassis.

Table 4-1. Summary of profiles and commands for monitoring interfaces

Device	Commands	Status profile
DS3-ATM trunk modules	`atmtrunks`	`ds3-atm-stat`
E3-ATM trunk module	`atmtrunks`	`e3-atm-stat`
OC3-ATM trunk module	`atmtrunks`	`oc3-atm-stat`
OC12-ATM trunk module		`sonet-stat`

Table 4-1. Summary of profiles and commands for monitoring interfaces (Continued)

Device	Commands	Status profile
Trunk aggregation module (TRAM)	`atmtrunks`	`oc3-atm-stat` `ds3-atm-stat`

8-port T1 module
24-port T1 module
8-port E1 module
24-port E1 module
	`imalines`
	`imagroups`
	`ima-tpp`
		`ima-group-stat`

All *x*DSL interfaces	`dsllines`	
Stinger MRT ADSL ports 12-port ADSL LIM 12-port Annex B DMT ADSL LIM 24-port DMT ADSL LIM 40-port ADSL Annex A LIM 48-port ADSL Annex A LIM 48-port ADSL Annex B LIM 48-port ADSL Annex C LIM 48-port G.lite ADSL LIM 72-port ADSL Annex A LIM (Globespan and Centillium)	`dmtaldsllines`	`al-dmt-stat`
32-port SHDSL/HDSL2 LIM	`hdsl2lines`	`hdsl2-stat`
48-port SHDSL LIM 72-port SHDSL LIM Stinger MRT SHDSL ports	`shdsllines`	`shdsl-stat`
48-port SDSL v1 LIM 48-port SDSL v2 LIM	`sdsllines`	`sdsl-stat`

Using profiles to monitor LIM and trunk interfaces

The Stinger unit creates a read-only status profile for each interface, which provides information about the status, redundancy settings, and statistical information for that interface. The following sections provide an overview of these profiles. For a detailed explanation of the parameters in these profiles and subprofiles, see the module configuration guide for your device or the *Stinger Reference*.

For example, a Stinger unit with a dual-port DS3-ATM trunk module and two 8-port T1 modules enabled for inverse multiplexing over ATM (IMA) has a status profile for each DS3 port and 16 status profiles for its T1 ports, as shown in the following examples.

```
admin> dir ds3-atm-stat
     0  02/14/2002 18:04:12  { shelf-1 trunk-module-1 1 }
     0  02/14/2002 18:04:12  { shelf-1 trunk-module-1 2 }
admin>  dir ds1-atm-stat
     0  02/09/2002 00:19:30  { shelf-1 slot-3 1 }
     0  02/09/2002 00:19:30  { shelf-1 slot-3 2 }
     0  02/09/2002 00:19:30  { shelf-1 slot-3 3 }
     0  02/09/2002 00:19:30  { shelf-1 slot-3 4 }
     0  02/09/2002 00:19:30  { shelf-1 slot-3 5 }
     0  02/09/2002 00:19:30  { shelf-1 slot-3 6 }
     0  02/09/2002 00:19:30  { shelf-1 slot-3 7 }
     0  02/09/2002 00:19:30  { shelf-1 slot-3 8 }
     0  02/09/2002 00:19:30  { shelf-1 slot-12 1 }
     0  02/09/2002 00:19:30  { shelf-1 slot-12 2 }
     0  02/09/2002 00:19:30  { shelf-1 slot-12 3 }
     0  02/09/2002 00:19:30  { shelf-1 slot-12 4 }
     0  02/09/2002 00:19:30  { shelf-1 slot-12 5 }
     0  02/09/2002 00:19:30  { shelf-1 slot-12 6 }
     0  02/09/2002 00:19:30  { shelf-1 slot-12 7 }
     0  02/09/2002 00:19:30  { shelf-1 slot-12 8 }
```

Monitoring trunk module interfaces

The `ds3-atm-stat`, `e3-atm-stat`, and `oc3-atm-stat` profiles show the physical address of the device, state of the line, redundancy settings, and error and statistic information specific to that trunk module.

The following sample commands display the `ds3-atm-stat` profile for one of the DS3 interfaces of a DS3-ATM trunk module installed in slot 17:

```
admin> read ds3-atm-stat {1 17 1}
DS3-ATM-STAT/{ shelf-1 trunk-module-1 1 } read
admin> list
[in DS3-ATM-STAT/{ shelf-1 trunk-module-1 1 }]
physical-address* = { shelf-1 trunk-module-1 1 }
line-state = active
spare-physical-address = { any-shelf any-slot 0 }
sparing-state = sparing-none
sparing-change-reason = manual
sparing-change-time = 0
sparing-change-counter = 0
vpi-vci-range = vpi-0-255-vci-32-8191
vc-switching-vpi = ""
vcc-vpi = [ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 ]
f-bit-error-count = 512
p-bit-error-count = 24
cp-bit-error-count = 16
feb-error-count = 37
bpv-error-count = 22475
ezd-error-count = 45648
corrected-hec-error-count = 0
uncorrected-hec-error-count = 0
loss-of-signal = False
```

```
loss-of-frame = False
yellow-receive = False
ais-receive = False
```

For additional information about these parameters, see the *Stinger Reference*.

Monitoring LIM interfaces

The LIM status profiles shown in Table 4-1 include parameters and subprofiles that report the following information for the line or port:

- Physical address.
- Status.
- Redundancy settings.
- Virtual path identifier (VPI) and virtual channel identifier (VCI) range.
- VPI setting for virtual channel switching.
- Error and statistic counters that are specific to that device.
- Information specific to a particular device. For example, the status profiles for the ADSL, SDSL, SHDSL, and SHDSL/HDSL2 LIMs include the following subprofiles:
  - `physical-status` subprofile, which includes information about line and modem status, firmware version, data rates, error counts, and operational mode for the interface.
  - `physical-statistics` subprofile, which includes information about signal presence, modem integrity, operational statistics, and error statistics for the interface.

  The T1 and E1 modules enabled for IMA include the following subprofiles:
  - `ima-link-status` subprofile, which provides information about the status of an IMA link
  - `ima-link-statistic` subprofile, which provides statistics for the IMA link.
  - `ima-group-stat` subprofile, which monitors the performance of an IMA group. This subprofile is created by the system automatically once the `imagroup` profile is properly configured and associated with a DS1-ATM profile.

The following sample commands display the `al-dmt-stat` profile for port 5 on a 24-port ADSL LIM installed in slot 2:

```
admin> read al-dmt-stat {1 2 5}
AL-DMT-STAT/{ shelf-1 slot-2 5 } read

admin> list
[in AL-DMT-STAT/{ shelf-1 slot-2 5 }]
physical-address* = { shelf-1 slot-2 5 }
line-state = active
spare-physical-address = { any-shelf any-slot 0 }
sparing-state = sparing-none
sparing-change-reason = unknown
sparing-change-time = 0
sparing-change-counter = 0
vpi-vci-range = vpi-0-15-vci-32-127
vp-switching-vpi = 15
```

```
physical-status = { 38 coe loopback 0 0 0 0 none none "069.8 " 2 1 10 init-ok
0+
physical-statistic = { { 0 0 0 } no 0 not-done 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 }
```

The following sample commands display the `ds1-atm-stat` profile for an IMA port on a 8-port T1 module installed in slot 3.

```
admin> read ds1-atm-stat {1 3 1}
DS1-ATM-STAT/{ shelf-1 slot-3 1 } read

admin> list
[in DS1-ATM-STAT/{ shelf-1 slot-3 1 }]
physical-address* = { shelf-1 slot-3 1 }
line-mode = uni
line-state = disabled
loss-of-carrier = yes
loss-of-sync = no
ais-receive = no
yellow-receive = no
ber-receive = no
carrier-established = no
cell-delineation = no
network-loopback = no
spare-physical-address = { any-shelf any-slot 0 }
sparing-state = sparing-none
sparing-change-reason = unknown
sparing-change-time = 0
sparing-change-counter = 0
vpi-vci-range = vpi-0-15-vci-32-127
vp-switching-vpi = 15
ima-link-status = { not-in-group not-in-group not-in-group not-in-group
no-fail+
ima-link-statistic = { 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 }
utopia-address = 4294967295
pattern-test-status = none
status-change-time-stamp = 0
```

For a discussion about the values reported by the parameters in the status profiles, see the module configuration guide for your device or the *Stinger Reference*.

Displaying interface information

You can use commands to display status information for the interfaces of the LIMs and trunks on a Stinger unit. The `dmtaldsllines`, `hdsl2lines`, `imalines`, `sdsllines`, `shdsllines`, `imagroups`, and `atmtrunks` commands display information about interfaces of a specific type in a Stinger unit.

For a description of a command's syntax, enter the command without any arguments. You use these commands with one of the following options:

Option	Description
`-a`	Displays information about all interfaces of a particular type.

Option	Description
`-d`	Displays all disabled interfaces of a particular type.
`-f`	Displays all available interfaces of a particular type.
`-u`	Displays all interfaces of a particular type that are in use.
`-c`	(Applicable to the atmtrunks command.) Clears trunk statistics for a specific port, slot or all trunk statistics for a Stinger unit.

The output from `dmtaldsllines`, `hdsl2lines`, `imalines`, `sdsllines`, `shdsllines`, `imagroups`, and `atmtrunks` commands displays the same fields. Table 4-2 lists the fields from the output of these commands.

Table 4-2. Field descriptions for status commands

Field	Indicates
(dvOp)	Operational state of the interface. `Down` indicates that the line is in a nonoperational state. `Up` indicates that the line is in normal operations mode.
(dvUpSt)	Status of the interface in normal operations mode. `Idle` indicates that no call is on the line. `Assign` indicates that the line is handling a call.
(dvRq)	Required state of the interface. `Down` indicates that the line is required to be nonoperational. `Up` indicates that the line is required to be in normal operations mode.
(sAdm)	Desired state of the interface. `Down` specifies that the interface should terminate all operations and enter the deactivated state. `Up` specifies that the line should be activated in normal operations mode.
(nailg)	Nailed-group number that this interface is assigned to
(Imode)	For T1 or E1 module only, the mode of operation: User-to-Network Interface (UNI) or IMA (`ATM`).

Displaying trunk port status

To display the status of the all trunk ports of a Stinger unit, use the `-a` option:

```
admin> atmtrunks -a
All OC3 ATM trunks:
                 OC3 Lines      (dvOp   dvUpSt  dvRq    sAdm    nailg)
  Line    {    1 17  1 }       (Up      Assign  UP      UP     00801)
  Line    {    1 17  2 }       (Up      Assign  UP      UP     00802)
  Line    {    1 18  1 }       (Up      Assign  UP      UP     00851)
  Line    {    1 18  2 }       (Down    Idle    DOWN    DOWN   00852)

All DS3 ATM trunks:
```

```
                  DS3 Lines       (dvOp   dvUpSt  dvRq    sAdm    nailg)
  Line    {    1 18  3 }         (Down    Idle    DOWN    DOWN   00853)
  Line    {    1 18  4 }         (Down    Idle    DOWN    DOWN   00854)
  Line    {    1 18  5 }         (Down    Idle    DOWN    DOWN   00855)
  Line    {    1 18  6 }         (Down    Idle    DOWN    DOWN   00856)

All E3 ATM trunks:
                  E3 Lines         (dvOp   dvUpSt  dvRq    sAdm    nailg)

All OC12  lines:
                                   (dvOp    dvUpSt  dvRq    sAdm   nailg)
```

To display the status of the all available trunk ports on a Stinger unit, use the **-f** option:

```
admin> atmtrunks -f
Disabled OC3 ATM trunks:
                  OC3 Lines       (dvOp   dvUpSt  dvRq    sAdm    nailg)
  Line    {    1 18  2 }         (Down    Idle    DOWN    DOWN   00852)

Disabled DS3 ATM trunks:
                  DS3 Lines       (dvOp   dvUpSt  dvRq    sAdm    nailg)
  Line    {    1 18  3 }         (Down    Idle    DOWN    DOWN   00853)
  Line    {    1 18  4 }         (Down    Idle    DOWN    DOWN   00854)
  Line    {    1 18  5 }         (Down    Idle    DOWN    DOWN   00855)
  Line    {    1 18  6 }         (Down    Idle    DOWN    DOWN   00856)

Disabled E3 ATM trunks:
                  E3 Lines         (dvOp   dvUpSt  dvRq    sAdm    nailg)

Disabled OC12 lines:
                                   (dvOp    dvUpSt  dvRq    sAdm   nailg)
```

To display all disabled trunk ports on a Stinger unit, use the **-d** option:

```
admin> atmtrunks -d
Disabled OC3 ATM trunks:
                  OC3 Lines       (dvOp   dvUpSt  dvRq    sAdm    nailg)
  Line    {    1 18  2 }         (Down    Idle    DOWN    DOWN   00852)

Disabled DS3 ATM trunks:
                  DS3 Lines       (dvOp   dvUpSt  dvRq    sAdm    nailg)
  Line    {    1 18  3 }         (Down    Idle    DOWN    DOWN   00853)
  Line    {    1 18  4 }         (Down    Idle    DOWN    DOWN   00854)
  Line    {    1 18  5 }         (Down    Idle    DOWN    DOWN   00855)
  Line    {    1 18  6 }         (Down    Idle    DOWN    DOWN   00856)

Disabled E3 ATM trunks:
                  E3 Lines         (dvOp   dvUpSt  dvRq    sAdm    nailg)

Disabled OC12 lines:
                                   (dvOp    dvUpSt  dvRq    sAdm   nailg)
```

To display all trunk ports that are in use, enter the command with the **-u** option:

```
admin> atmtrunks -u
```

```
In-Use OC3 ATM trunks:
                 OC3 Lines       (dvOp   dvUpSt  dvRq    sAdm    nailg)
  Line    {    1 17  1 }        (Up      Assign  UP      UP     00801)
  Line    {    1 17  2 }        (Up      Assign  UP      UP     00802)
  Line    {    1 18  1 }        (Up      Assign  UP      UP     00851)

In-Use DS3 ATM trunks:
                 DS3 Lines       (dvOp   dvUpSt  dvRq    sAdm    nailg)

In-Use E3 ATM trunks:
                 E3 Lines         (dvOp   dvUpSt  dvRq    sAdm    nailg)

In-Use OC12 lines:
                                 (dvOp    dvUpSt  dvRq    sAdm   nailg)
```

Resetting trunk statistics

To reset the trunk statistics for OC3-ATM and DS3-ATM trunk modules, use the `-c` option. The following example clears trunk statistics for all trunks:

```
admin> atmtrunks -c
Clearing ATM Trunk Statistics for All Trunks
```

The following example clears trunk statistics for a specific slot:

```
admin> atmtrunks -c 17
Clearing ATM Trunk Statistics for Slot 17
```

Displaying LIM interfaces

Following are sample commands that display information about interfaces of different LIMs.

Displaying ADSL LIM interfaces

The following sample `dmtaldsllines` commands shows information about the ADSL interfaces of a Stinger unit with a 48-port ADSL LIM in slot 3 and slot 11, and a 24-port ADSL LIM in slot 5.

The `dmtaldsllines -a` command displays the status and nailed group information for all ADSL ports in the Stinger unit. The output of the following command is abbreviated.

```
admin> dmtaldsllines -a
                                  (dvOp   dvUpSt  dvRq    sAdm    nailg)
  Line    {    1  3  1 }        (Down    Idle    DOWN    DOWN   00101)
  Line    {    1  3  2 }        (Down    Idle    DOWN    DOWN   00102)
  Line    {    1  3  3 }        (Down    Idle    DOWN    DOWN   00103)
  ...
  ...
  ...
  Line    {    1  3 46 }        (Down    Idle    DOWN    DOWN   00146)
  Line    {    1  3 47 }        (Down    Idle    DOWN    DOWN   00147)
  Line    {    1  3 48 }        (Down    Idle    DOWN    DOWN   00148)
  Line    {    1  5  1 }        (Down    Idle    DOWN    DOWN   00201)
  Line    {    1  5  2 }        (Up      Assign  UP      UP     00202)
```

```
  Line    {    1  5  3 }        (Up      Assign  UP      UP     00203)
  ...
  ...
  ...
  Line    {    1  5 22 }        (Down    Idle    DOWN    DOWN   00222)
  Line    {    1  5 23 }        (Down    Idle    DOWN    DOWN   00223)
  Line    {    1  5 24 }        (Down    Idle    DOWN    DOWN   00224)
  Line    {    1 11  1 }        (Down    Idle    DOWN    DOWN   00501)
  Line    {    1 11  2 }        (Down    Idle    DOWN    DOWN   00502)
  Line    {    1 11  3 }        (Down    Idle    DOWN    DOWN   00503)
  ...
  ...
  ...
  Line    {    1 11 46 }        (Down    Idle    DOWN    DOWN   00546)
  Line    {    1 11 47 }        (Down    Idle    DOWN    DOWN   00547)
  Line    {    1 11 48 }        (Down    Idle    DOWN    DOWN   00548)
```

The following sample command displays all available ADSL lines in the Stinger unit:

```
admin> dmtaldsllines -f
Free DMT ADSL lines:
                                (dvOp   dvUpSt  dvRq    sAdm    nailg)
  Line    {    1  3  5 }        (Up      Idle    UP      UP     00051)
  Line    {    1  5  1 }        (Up      Idle    UP      UP     00301)
```

The following sample command displays all disabled ADSL lines in the Stinger unit:

```
admin> dmtaldsllines -d
Disabled DMT ADSL lines:
                                (dvOp   dvUpSt  dvRq    sAdm    nailg)
  Line    {    1  2  2 }        (Down    Idle    DOWN    DOWN   00052)
  Line    {    1  2  3 }        (Down    Idle    DOWN    DOWN   00053)
  Line    {    1  2  4 }        (Down    Idle    DOWN    DOWN   00054)
  Line    {    1  2  5 }        (Down    Idle    DOWN    DOWN   00055)
```

The following sample command displays all the ADSL lines that are in use.

```
admin> dmtaldsllines -u
                                (dvOp   dvUpSt  dvRq    sAdm    nailg)
  Line    {    1  5  2 }        (Up      Assign  UP      UP     00202)
  Line    {    1  5  3 }        (Up      Assign  UP      UP     00203)
```

Displaying T1 and E1 interfaces

The following sample command displays information about the T1 modules installed in slot 4 and slot 6:

```
admin> imalines -a
All IMA lines:
                                (dvOp  dvUpSt  dvRq   sAdm  lMode  Nailg)
 Line  {   1  4  1 }           (Up     Assign UP     UP     ATM   00151)
 Line  {   1  4  2 }           (Down   Idle   DOWN   DOWN   ATM   00152)
 Line  {   1  4  3 }           (Down   Idle   DOWN   DOWN   ATM   00153)
 Line  {   1  4  4 }           (Down   Idle   DOWN   DOWN   ATM   00154)
 Line  {   1  4  5 }           (Down   Idle   DOWN   DOWN   ATM   00155)
 Line  {   1  4  6 }           (Down   Idle   DOWN   DOWN   ATM   00156)
```

```
Line  {   1  4  7 }          (Down   Idle   DOWN   DOWN   ATM   00157)
Line  {   1  4  8 }          (Down   Idle   DOWN   DOWN   ATM   00158)
Line  {   1  4  9 }          (Down   Idle   DOWN   DOWN   ATM   00159)
Line  {   1  4 10 }          (Down   Idle   DOWN   DOWN   ATM   00160)
Line  {   1  4 11 }          (Down   Idle   DOWN   DOWN   ATM   00161)
Line  {   1  4 12 }          (Down   Idle   DOWN   DOWN   ATM   00162)
Line  {   1  4 13 }          (Down   Idle   DOWN   DOWN   ATM   00163)
Line  {   1  4 14 }          (Down   Idle   DOWN   DOWN   ATM   00164)
Line  {   1  4 15 }          (Down   Idle   DOWN   DOWN   ATM   00165)
Line  {   1  4 16 }          (Down   Idle   DOWN   DOWN   ATM   00166)
Line  {   1  4 17 }          (Down   Idle   DOWN   DOWN   ATM   00167)
Line  {   1  4 18 }          (Down   Idle   DOWN   DOWN   ATM   00168)
Line  {   1  4 19 }          (Down   Idle   DOWN   DOWN   ATM   00169)
Line  {   1  4 20 }          (Down   Idle   DOWN   DOWN   ATM   00170)
Line  {   1  4 21 }          (Down   Idle   DOWN   DOWN   ATM   00171)
Line  {   1  4 22 }          (Down   Idle   DOWN   DOWN   ATM   00172)
Line  {   1  4 23 }          (Down   Idle   DOWN   DOWN   ATM   00173)
Line  {   1  4 24 }          (Down   Idle   DOWN   DOWN   ATM   00174)
Line  {   1  6  1 }          (Up     Assign UP     UP     ATM   00251)
Line  {   1  6  2 }          (Up     Assign UP     UP     ATM   00252)
Line  {   1  6  3 }          (Up     Assign UP     UP     ATM   00253)
Line  {   1  6  4 }          (Up     Assign UP     UP     ATM   00254)
Line  {   1  6  5 }          (Up     Assign UP     UP     ATM   00255)
Line  {   1  6  6 }          (Up     Assign UP     UP     ATM   00256)
Line  {   1  6  7 }          (Up     Assign UP     UP     ATM   00257)
Line  {   1  6  8 }          (Up     Assign UP     UP     ATM   00258)
```

Displaying IMAgroups

The `imagroups` command displays the status of IMA groups that have been created, or those that are in use, free, or disabled on T1 or E1 modules in a Stinger unit. For example:

```
admin> imagroups -a
All IMA groups:
                                (dvOp   dvUpSt  dvRq    sAdm       nailg)
     ima101 {  1  3  9 }        (Down    Idle    UP      UP          101)
```

Testing IMA connectivity

To initiate a test pattern procedure that can detect misconfigured IMA connections, according to ATM Forum IMA specifications, use the `ima-tpp` command. For syntax information, see the *Stinger Reference*.

The following sample command initiates test pattern 200 on link 7 in IMA group `ima3_4` and requests a report of test results:

```
admin> ima-tpp ima3_4 7 200 yes yes
IMA TPP request sent, please wait for a response ...
admin> TPP test result:

ImaGroupName=ima3_4, ImaTppTestResult=TPP_PASSED
2 links configured in IMA group ima3_4, all passed TPP test!
```

Monitoring LIM and LIM port redundancy

You can configure a redundant line interface module (LIM) that you can manually activate—or configure a Stinger unit to automatically activate—when a previously active LIM or LIM port goes offline.

A fast-restore capability enables Stinger units with redundant control modules to restore the data path of cross-connections within about 10 seconds following a failover of the primary control module. The fast-restore operation restores the data path of cross-connections (virtual circuits that use `atm-circuit` encapsulation) in the application-specific integrated circuit (ASIC) switching fabric while TAOS call-control mechanisms are reestablishing connections.

Terminating connections (virtual circuits that use `atm` encapsulation), OAM data paths, and soft permanent virtual circuits (SPVCs) are not affected by the fast-restore operation. Those connections are reestablished in the usual time frame via TAOS call control.

For configuration instructions for redundant LIMs and ports, see the module guide for your particular device.

To determine the status of LIMs and ports configured for redundancy, use the following profiles and commands:

- `lim-sparing-status` profile and numbered subprofiles, which indicate redundancy status on the Stinger unit and the current configuration
- Individual LIM line status profiles, which indicate port redundancy status for the selected port and information about the spare LIM
- `rearslot` command
- `splimports` command

Overview of port redundancy parameters

The status profile for each interface indicates whether redundancy is enabled and provides other useful information about the status of the redundancy function on a LIM (see "Using profiles to monitor LIM and trunk interfaces" on page 4-2). Following is an overview of the parameters that report redundancy information.

Parameter	Specifies
`spare-physical-address`	Shelf, slot, and port number of spare LIM.
`sparing-state`	State of the redundancy function. If redundancy is not enabled, `sparing-none` is the value. If redundancy is enabled and the LIM slot contains a primary LIM, the value can be `primary-active` or `primary-inactive`. If redundancy is enabled and the LIM slot contains the secondary LIM, the value can be `secondary-active` or `secondary-inactive`.
`sparing-change-reason`	How redundancy is activated. Valid values are `inactive`, `manual`, and `automatic`.
`sparing-change-time`	Time that the last change in redundancy state occurred.

Parameter	Specifies
sparing-change-counter	Number of redundancy changes (for example, primary to secondary or secondary to primary). The counter is reset to zero each time the Stinger unit is turned on.

Verifying port redundancy status

The following sample commands display the redundancy status an active line on an SDSL LIM:

```
admin> read sdsl-stat { 1 4 6}
SDSL-STAT/{ shelf-1 slot-4 6 } read

admin> list
[in SDSL-STAT/{ shelf-1 slot-4 6 }]
.....
spare-physical-address = { shelf-1 slot-16 6 }
sparing-state = primary-inactive
sparing-change-reason = manual
sparing-change-time = 309108872
sparing-change-counter = 1
.....
```

Verifying slot configuration redundancy status

The `rearslotshow` command shows the status of all slots used for line protection modules (LPMs), path selector modules (PSMs), and copper loop test (CLT) modules. It also reports on the status of the midplane sparing bus.

For example, suppose that a Stinger FS is equipped with ADSL LIMs and SDSL LIMs. The 24-port ADSL LIM in slot 1 has failed and is being replaced by the 24-port ADSL LIM in slot 14. The `rearslotshow` command reports the following.

```
admin> rearslotshow
[ 1 ] 91 24 port Enhanced LPM
[ 2 ] 0 Empty ( IRM, LPM )
[ 3 ] 0 Empty ( IRM, LPM )
[ 4 ] 92 48 port Enhanced LPM)
[ 5 ] 0 Empty ( IRM, LPM )
[ 6 ] 0 Empty ( IRM, LPM )
[ 7 ] 0 Empty ( IRM, LPM )
[ 10 ] 0 Empty ( IRM, LPM )
[ 11 ] 0 Empty ( IRM, LPM )
[ 12 ] 0 Empty ( IRM, LPM )
[ 13 ] 0 Empty ( IRM, LPM )
[ 14 ] 93 Path Selector Module ( PSM )
[ 15 ] 0 Empty ( IRM, LPM )
[ 16 ] 94 Copper Loop Tester ( CLT )

 Midplane sparing bus usage :

   7            6           5            4  3
 2109 8765 4321 0987 6543 2109 8765 4321 0987
 .... .... .... .... .... .... .... .... ....
```

```
       3           2           1
6543 2109 8765 4321 0987 6543 2109 8765 4321
.... .... .... .... .... .... .... .... ....
Test Bus usage : not applicable
```

Note Slots that are equipped with interface redundancy modules (IRMs) or LPMs with redundancy (LPM-Rs) in older Stinger units are reported as `Empty` by the `rearslotshow` command.

Note When a copper loop is being tested on a Stinger LS with a PSM or a CLT module, the `rearslotshow` command does not display any midplane sparing bus usage.

Displaying redundancy or ignore-lineup settings for LIM ports

The `splimports` command displays ports that are enabled for automatic or manual redundancy or the ignore-lineup feature. (This feature allows the unit to accept calls on a port whether the line state is UP or DOWN, as long as the slot is operational and the port is enabled.) To display syntax information, enter the command without any arguments or see the *Stinger Reference*.

The following sample command displays ports in slot 7 that are enabled with the system-wide setting for the ignore-lineup feature:

```
admin> splimports -i -s 7
Line            Type
--------------------
1-7-2           ADSL
1-7-7           ADSL
1-7-11          ADSL
...
...
...
1-7-22          ADSL
1-7-23          ADSL
1-7-24          ADSL
```

The following sample command displays all ports that are disabled for the ignore-lineup feature:

```
admin> splimports -i -n
Line            Type
--------------------
1-7-1           ADSL
1-7-4           ADSL
1-7-5           ADSL
1-7-6           ADSL
1-7-9           ADSL
1-7-14          ADSL
1-16-21         HDSL2
1-16-22         HDSL2
1-16-23         HDSL2
```

The following sample command displays all ports that are configured for automatic or manual redundancy:

```
admin> splimports -s
Line            Type        Sparing Mode
---------------------------------------
1-3-1           SDSL        Manual
1-3-2           SDSL        Auto
1-3-3           SDSL        Manual
1-7-4           ADSL        Auto
1-7-5           ADSL        Manual
1-7-6           ADSL        Auto
```

The following sample command displays ports that are configured for automatic redundancy:

```
admin> splimports -s -a
Line            Type        Sparing Mode
---------------------------------------
1-3-2           SDSL        Auto
1-7-4           ADSL        Auto
1-7-6           ADSL        Auto
```

Monitoring redundant trunk groups

To display information about the Stinger unit's trunk port redundancy operations, use the `-s` option with the `atmtrunks` command. The following sample command shows the output of the `atmtrunks -s` command, followed by field descriptions.

```
admin> atmtrunks -s
 Group   Primary         Sparing         State   SparingChangeTime
     1   18 -  1         17 -  1         Auto_S  410719627
```

Field	Specifies
`Group`	Trunk group number.
`Primary`	Slot number and trunk interface number of the primary trunk port.
`Sparing`	Slot number and trunk interface number of the redundant trunk port.
`State`	State of the trunk port redundancy operations. Values can be one of the following: ■ `InAct`—Trunk port redundancy is disabled. ■ `Manu`—Trunk port redundancy is in manual mode. ■ `Auto_S`—Automatic trunk port redundancy is enabled and the redundant trunk port is active. ■ `Auto_P`—Automatic trunk port redundancy is enabled and the primary trunk port is active.
`SparingChangeTime`	Timestamp for when the trunk port redundancy operation last occurred.

Working with IP Traffic

5

The following TCP/IP information and commands apply to any interface with an IP address. The Stinger unit maintains an internal IP routing table. You can configure the system to use RIP to propagate the information in that table to other routers, receive information from other routers, or both, on any LAN or WAN interface.

TAOS supports commands that are useful for locating the sources of problems on the network and for communicating with other hosts for management purposes.

For complete information about the commands described in this chapter, see the *Stinger Reference*.

Testing IP connectivity

The `ping` command is useful for verifying that the transmission path between the Stinger unit and another station is open. Ping sends an ICMP Echo-Request packet to the specified station. If the station receives the packet, it returns an ICMP Echo-Response packet. For example, to ping the host `techpubs`:

```
admin> ping techpubs
PING techpubs (10.65.212.19): 56 data bytes
```

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

To terminate the ping exchange at any time, press Ctrl-C. When you press Ctrl-C, the system reports the number of packets sent and received, the percentage of packet loss, the number of duplicate or damaged Echo-Response packets (if any), and round-trip statistics. In some cases, round-trip times cannot be calculated.

During the ping exchange, the Stinger unit displays information about the packet exchange, including the time-to-live (TTL) of each ICMP Echo-Response packet.

The maximum TTL for ICMP ping is 255, but the maximum TTL for TCP is often 60 or lower, so you might be able to ping a host but not be able to run a TCP application (such as Telnet or FTP) to that station. If you ping a host running a version of Berkeley UNIX before 4.3BSD-Tahoe, the TTL report is 255 minus the number of routers in the round-trip path. If you ping a host running the current version of Berkeley UNIX, the TTL report is 255 minus the number of routers in the path from the remote system to the station performing the ping.

The `ping` command also supports the `-f` option, which sets the Don't Fragment (DF) bit in the IP header of ping packets. Setting the DF bit enables the Stinger unit to discover the datagram size, or *path maximum transmission unit (PMTU)*, of the path from the remote host. If any datagram is too large to be forwarded without fragmentation by some router along the path, the router discards it and returns an ICMP `Destination Unreachable` message with a code indicating `that fragmentation is needed and the DF bit is set`.

For example, the following command sends an ICMP packet to host 10.1.1.1, with the DF bit set:

```
admin> ping -f 10.1.1.1
```

For more information, see RFC 1191, *Path MTU Discovery*, and RFC 2401, *Security Architecture for the Internet Protocol*.

Displaying the IP interface table

At system startup, the Stinger unit creates an IP interface in the active state for each Ethernet interface that has a configured `ip-interface` profile and for built-in loopback, reject, and blackhole interfaces. It also creates IP interfaces in the inactive state for remote connections.

For each IP interface that is not configured as a private route, the system also adds a route to the routing table.

IP interfaces change between the active and inactive state as switched calls are established and ended. To display the interface table, enter the `netstat` command with the `-in` option, as in the following example:

```
admin> netstat -i
Name       MTU   Net/Dest          Address         Ipkts    Ierr Opkts    Oerr
ie0         1500 134.112.26.0/24   134.112.26.201  1050443    0    47540    0
lo0         1500 127.0.0.1/32      127.0.0.1         47504    0    47504    0
```

```
rj0          1500 127.0.0.2/32       127.0.0.2             0    0        0    0
bh0          1500 127.0.0.3/32       127.0.0.3             0    0        0    0
wanabe       1500 127.0.0.3/32       127.0.0.3             0    0        0    0
local       65535 127.0.0.1/32       127.0.0.1        295498    0   295498    0
mcast       65535 224.0.0.0/4        224.0.0.0        134037    0   134037    0
tunnel0      1500 134.112.26.0/24    134.112.26.201        0    0        0    0
vr0_main     1500 134.112.26.201/32  134.112.26.201        0    0        0    0
sip0        65535 -                  -                     0    0        0    0
ie1-2-1      1500 -                  -                     0    0        0    0
ie1-2-2      1500 -                  -               1008273    0        0    0
wan26        1560 222.222.222.2      222.222.222.1     12893    0      391    0
```

The interface table contains the following information:

Column	Indicates
Name	Name of the interface: ■ ie0-*n* —The control module Ethernet interfaces. ■ lo0—The loopback interface. ■ rj0—The reject interface, used in network summarization. ■ bh0—The blackhole interface, used in network summarization. ■ wanN —A WAN connection, entered as it becomes active. ■ wanabe—An inactive RADIUS dial-out profile. ■ local—The local machine.
MTU	Maximum transmission unit. The maximum packet size allowed on the interface.
Net/Dest	Network or the target host this interface can reach.
Address	Address of this interface.
Ipkts	Number of packets received.
Ierr	Number of packets that contain errors.
Opkts	Number of packets transmitted.
Oerr	Number of transmitted packets that contain errors.

Displaying and modifying IP routes

You can use the `netstat` command to display the IP routing table. To add or delete static routes, use the `iproute` command.

Using the `netstat` command to display the IP routing table

To display the routing table, enter the `netstat` command with the `-r` argument, as in the following example:

```
admin> netstat -r
Destination       Gateway        IF         Flg   Pref Met     Use       Age
0.0.0.0/0         134.112.26.1   ie0        SGP     60   1   60264    507191
```

```
127.0.0.0/8        -               bh0         CP       0   0       0     669778
127.0.0.1/32       -               local       CP       0   0       3     669778
127.0.0.2/32       -               rj0         CP       0   0       0     669778
134.112.26.0/24    -               ie0         C        0   0   52758     669778
134.112.26.201/32  -               local       CP       0   0   18312     669778
222.222.222.1/32   -               local       rT       0   0       4     507191
222.222.222.2/32   222.222.222.2   wan26       rT      60   1       4     507191
224.0.0.0/4        -               mcast       CP       0   0    2837     669778
224.0.0.1/32       -               local       CP       0   0       0     669778
224.0.0.2/32       -               local       CP       0   0       0     669778
224.0.0.9/32       -               local       CP       0   0       0     669778
255.255.255.255/32 -               ie0         CP       0   0   63605     669778
Total Routes  = 13      Hidden Routes = 0
```

The columns in the routing table contain the following information:

Column	Indicates
`Destination`	Route's target address. To send a packet to this address, the Stinger unit uses this route. If the target address appears more than once in the routing table, the Stinger unit uses the most specific route (having the largest subnet mask) that matches that address.
`Gateway`	Next-hop router that can forward packets to the given destination. Direct routes (without a gateway) show a hyphen in this column.
`IF`	Name of the interface through which to send packets over this route. For an explanation of available interface types, see the *Stinger Reference*.
`Flg`	Means by which the route was added to the table. For example, the *R* flag indicates that the route was learned from RIP, and the *S* flag indicates a statically defined route. For an explanation of available flag types see the *Stinger Reference*.
`Pref`	Preference value for the route. When choosing a route, the system first compares their preference values, preferring the lowest number. For more information about the defaults for route preferences, see the description of the `preference` parameter in the *Stinger Reference*.
`Metric`	RIP-style metric for the route, with a range of 0 through 16.
`Use`	Number of times the route was referred to since it was created. (Many of these references are internal, so this value is not a count of the number of packets sent over this route.)
`Age`	Age of the route in seconds. RIP and ICMP entries are aged once every 10 seconds.

Modifying the IP routing table

The `iproute` command enables you to manually add routes to the routing table, delete them, or change their preference or metric values. The command is useful for temporary routing changes. Changes that you make to the routing table with the `iproute` command are valid only until you reset the Stinger system or remove power

to the unit. RIP updates can add back any route that you remove using the `iproute delete` command. Also, the Stinger unit restores all routes listed in the `ip-route` profile after you reset the unit.

For syntax information, see the *Stinger Reference*.

Adding a static IP route to the routing table

To add a static IP route to the Stinger unit's routing table, use the `iproute add` command.

For example, the following command adds a route to the network 10.1.2.0 and all its subnets through the IP router located at 10.0.0.3/24. The metric to the route is 1 (one hop away).

```
admin> iproute add 10.1.2.0/24 10.0.0.3/24 1
```

If you try to add a route to a destination that is already in the routing table, the Stinger unit does not replace the existing route unless it has a higher metric than the route you attempted to add. If you get the message `Warning: a better route appears to exist`, the Stinger unit has rejected your attempt to add a route.

Deleting a static IP route from the routing table

To remove a static IP route from the Stinger unit's routing table, enter the `iproute delete` command. The arguments are the same as for the `iproute add` command. For example, the following command removes the route to the 10.1.2.0 network:

```
admin> iproute delete 10.1.2.0 10.0.0.3/24
```

You can also change the metric or preference value of an existing route by using the `iproute` command. For example, suppose the routing table contains the following route:

```
Destination     Gateway     IF    Flg  Pref Met     Use       Age
10.122.99.0/24  10.122.99.1 wan4  SG   100   7       0        48630
```

You can change the preference from 100 to 50 and the metric from 7 to 3 as follows:

```
admin> iproute add 10.122.99.0/24 10.122.99.1 50 3
```

Tracing IP routes

The `traceroute` command is useful for locating slow routers or diagnosing IP routing problems. It traces the route an IP packet takes by launching UDP probe packets with a low time-to-live (TTL) value and then listening for an ICMP `time exceeded` reply from a router. For example, the following sample command traces the route to the host `techpubs`:

```
admin> traceroute techpubs

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

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

- The Stinger unit receives an ICMP `port unreachable` message. (The UDP port in the probe packets is set to an unlikely value, such as 33434, because the target host is not intended to process the packets. A `port unreachable` message indicates that the packets reached the target host and were rejected.)

- The TTL value reaches the maximum value. (By default, the maximum TTL is set to 30.) You can use the `-m` option to specify a different TTL. For example:

```
admin> traceroute -m 60 techpubs
traceroute to techpubs (10.65.212.19), 60 hops max, 0 byte packets
1  techpubs.abc.com (10.65.212.19)  0 ms  0 ms  0 ms
```

The `traceroute` command sends three probes at each TTL setting. The second line of output shows the address of the router and the round-trip time of each probe. If the probe answers come from different gateways, the address of each responding system is shown. If there is no response within a 3-second timeout interval, the second line of output is an asterisk.

For the details of the `traceroute` command, see the *Stinger Reference*.

Displaying IP protocol statistics

The `netstat` command displays the Stinger IP interface and routing tables, protocol statistics, and active sockets. By default (without an argument), the `netstat` command reports information about UDP and TCP socket information. For an explanation of the output fields, see the *Stinger Reference*.

```
admin> netstat
udp:
-Socket-  Local Port  InQLen  InQMax    InQDrops    Total Rx
1/c    0        1023       0       1           0           0
1/c    1         520       0       0           0       15510
1/c    2           7       0      32           0           0
1/c    3         123       0      32           0           0
1/c    4        5150       0     256           0           0
1/c    5        1022       0     128           0           0
1/c    6         161       0      32           0           0
1/c    7        1797       0     128           0          22
1/8    0        1018       0     128           0           0
1/8    1       20108       0      32           0           0
1/8    2        1008       0     128           0           0
1/8    3        1798       0     128           0           0
1/9    0        1021       0     128           0           0
1/9    1       20109       0      32           0           0
1/9    2        1009       0     128           0           0
1/9    3        1799       0     128           0           0
1/10   0        1020       0     128           0           0
1/10   1       20110       0      32           0           0
1/10   2        1010       0     128           0           0
1/10   3        1800       0     128           0           0
1/11   0        1017       0     128           0           0
1/11   1       20111       0      32           0           0
1/11   2        1011       0     128           0           0
1/11   3        1801       0     128           0           0
1/12   0        1019       0     128           0           0
1/12   1       20112       0      32           0           0
1/12   2        1012       0     128           0           0
1/12   3        1802       0     128           0           0
```

```
tcp:
-Socket- Local                      Remote                     State
1/c    0 192.168.7.135.79           *.*                        LISTEN
1/c    1 192.168.7.135.1723         *.*                        LISTEN
1/c    2 192.168.7.135.23           *.*                        LISTEN
1/c    4 192.168.7.135.23           172.20.32.137.42863        ESTABLISHED
1/c    9 192.168.7.135.23           206.65.212.10.1991         ESTABLISHED
```

The output shows the queue depth of various UDP ports, as well as the total packets received and total packets dropped on each port. The total-packets-received count includes the total packets dropped. For an explanation of the preceding output, see the *Stinger Reference*.

To displays the protocol statistics, use the the `-s` option. If no identifiers follow the `-s` option, the system shows all protocol statistics. For example:

```
admin> netstat -s
udp:
        15636 packets received
        0 packets received with no ports
        0 packets received with errors
        0 packets dropped
        68 packets transmitted

tcp:
        0 active opens
        7 passive opens
        0 connect attempts failed
        0 connections were reset
        2 connections currently established
        1457 segments received
        0 segments received out of order
        1728 segments transmitted
        18 segments retransmitted
        5 active closes
        0 passive closes
        0 disconnects while awaiting retransmission

icmp:
        216 packets received
        0 packets received with errors
        Input histogram:
                216 echo requests
        271 packets transmitted
        0 packets not transmitted due to lack of resources
        Output histogram:
                216 echo replies
                24 destination unreachable
                31 time exceeded

ip:
        28860 packets received
        0 packets received with header errors
        0 packets received with address errors
```

```
        0 packets received forwarded
        0 packets received with unknown protocols
        0 inbound packets discarded
        17310 packets delivered to upper layers
        2084 transmit requests
        0 discarded transmit packets
        49 outbound packets with no route
        0 reassemblies timeout
        268 reassemblies required
        12 reassemblies succeeded
        244 reassemblies failed
        12 fragmentation succeeded
        0 fragmentation failed
        24 fragmented packets created
        0 route discards due to lack of memory
        64 default ttl

igmp:
        0 packets received
        0 bad checksum packets received
        0 bad version packets received
        0 query packets received
        0 leave packets received
        0 packets transmitted
        0 query packets sent
        0 response packets sent
        0 leave packets sent

mcast:
        0 packets received
        0 packets forwarded
        0 packets in error
        0 packets dropped
        0 packets transmitted
```

To filter the type of protocol statistics displayed by the `netstat -s` command, add one of the following values to the `netstat -s` command: `udp`, `tcp`, `icmp`, `ip`, `igmp`, or `mcast`.

Displaying IP route cache information

The `ipcache` command displays information about IP route caches. A route cache enables a module to route IP packets to another slot, reducing the route-processing overhead on the control module. The control module is still responsible for managing routing protocols and the route caches themselves, but each module can check a small IP cache and route packets to a destination slot. When a module receives an IP packet for which it has no cache entry, it forwards that packet to the control module. The control module routes it to the proper slot and writes a cache entry. The cache entry is downloaded to the route cache of all modules via the control bus.

The command uses the following syntax:

`ipcache` [**`-r`** ***`vroutername`***] **`cache`**|**`debug`**|**`disable`**|**`enable`**

The following example shows command output on the control module:

```
admin> ipcache cache
Hsh     Address        Gateway        Ifname    Sh/Sl/T   MTU
20      50.0.0.20      10.168.26.74   wan392    1/14/D    1524
40      20.0.0.40      20.0.0.40      ie1-3-1   1/3 /S    1500
Cache Limit 0 Cache Count 2 Cache over limit 0 No.packets 9

Mem Usage: Allocated 1k bytes
Free block count 22
```

The following sample commands display output on a module:

```
admin> open 1 3
ether2-1/3> ipcache cache
Hsh Address    Gateway        Sh/Sl/T Switched  MTU    MPath
0   99.1.1.1   10.168.21.30   1/14/D  0         1524   Y/0.0.0.0/0
20  50.0.0.20  10.168.28.170  1/15/D  85068     1524   Y/0.0.0.0/0
40  20.0.0.40  20.0.0.40      1/3 /S  0         1500   N
Cache Limit 0 Cache Count 2 Cache over limit 0 No.packets 9
Mem Usage: Allocated 1k bytes
Free block count 22
```

The shelf number is always 1. The T (Type) column following the shelf and slot numbers can specify D for dynamic cache entries or S for static cache entries. The MPath column indicates whether the cache entry is derived from multipath routes. If it represents a multipath route, the column indicates Y and the destination address. If it is not a multipath route, the column indicates N.

Verifying name service settings

You can retrieve a host address by using the nslookup command, provided that the Stinger unit has been configured with the address of a name server. If a host has several IP interfaces, the command returns several addresses.

To retrieve the IP address of the host techpubs, proceed as in the following example:

```
admin> nslookup techpubs
Resolving host techpubs.
IP address for host techpubs is 10.65.212.19.
```

Displaying the ARP cache

The Address Resolution Protocol (ARP) translates between IP addresses and media access control (MAC) addresses as defined in RFC 826. Hosts broadcast an ARP request that is received by all hosts on the local network, and the one host that recognizes its own IP address sends an ARP response with its MAC address.

The Stinger unit maintains a cache of known IP addresses and host MAC addresses.

With the arptable command, you can display the ARP table, add or delete ARP table entries, or clear the ARP cache entirely. To display the ARP cache, enter the arptable command without any arguments, as in the following example:

```
admin> arptable
IP Address   MAC Address      Type IF Retries/Pkts/RefCnt TimeStamp
10.103.0.141 00:B0:24:BE:D4:84 DYN 0    0/0/1              23323
```

```
10.103.0.2   00:C0:7B:7A:AC:54 DYN 0    0/0/599          23351
10.103.0.220 00:C0:7B:71:83:02 DYN 0    0/0/2843         23301
10.103.0.1   08:00:30:7B:24:27 DYN 0    0/0/4406         23352
10.103.0.8   00:00:0C:06:B3:A2 DYN 0    0/0/6640         23599
10.103.0.7   00:00:0C:56:57:4C DYN 0    0/0/6690         23676
10.103.0.49  00:B0:80:89:19:95 DYN 0    0/0/398          23674
```

The ARP table displays the following information:

Field	Indicates
IP Address	Address contained in ARP requests.
MAC Address	MAC address of the host.
Type	How the address was learned, dynamically (DYN) or by specification of a static route (STAT).
IF	Interface on which the Stinger received the ARP request.
Retries	Number of retries needed to refresh the entry after it timed out.
Pkts	Number of packets sent out to refresh the entry after it timed out.
RfCnt	Number of times the Stinger unit consulted the entry.
TimeStamp	Number of seconds since the system was activated. The system updates this column every time an ARP table entry is refreshed.

To add an ARP table entry, use the **-a** option, as in the following example:

```
admin> arptable -a 10.65.212.3 00:00:81:3D:F0:48
```

To delete an ARP table entry, use the **-d** option, as in the following example:

```
admin> arptable -d 10.9.8.20
```

To clear the entire ARP table, use the **-f** option:

```
admin> arptable -f
```

Displaying the DNS host table

The local Domain Name System (DNS) host table supplies host IP addresses when DNS fails to successfully resolve a hostname. For information about configuring the DNS host table, see the *Stinger T1000 Module Routing and Tunneling Supplement*.

The DNS host table is not a DNS cache, but a fallback option, listing up to eight host addresses for important or frequently used connections. If you use the command without any options, the system displays the usage summary. To display the DNS host table, use the **-s** option. For example:

```
admin> dnstab -s
Local DNS Table:enabled, AutoUpdate: enabled.
Local DNS Table
 Name                IP Address      # Reads Time of last read
 1: "barney"         200.65.212.12 *  2      Feb 10 10:40:44 01
```

```
2: "rafael"         200.65.212.23    3      Feb 10  9:30:00 01
3: "donatello"      200.65.212.67    1      Feb 11 11:41:33 01
4: "wheelers"       200.65.212.9     1      Feb 12  8:35:22 01
```

The output of this commands contains the following fields:

Field	Indicates
`Local DNS Table`	Whether `enabled` is set to `yes` in the `ip-global:dns-local-table` subprofile.
`AutoUpdate`	Whether `auto-update` is set to `yes` in the `ip-global:dns-local-table` subprofile.
`Name`	Hostname.
`IP address`	IP address. An asterisk (*) indicates that the entry has been automatically updated by a DNS query.
`# Reads`	Number of accesses since the entry was created.
`Time of last read`	Time and date the entry was last accessed. If the Simple Network Time Protocol (SNTP) is not in use, the field contains hyphens.

You can also display a specific entry from the DNS table, using the syntax `dnstab` *`entry number`*, where *`entry number`* is the number of an entry in the DNS table.

Displaying the Ethernet information

The following commands provide information about Ethernet packets.

Displaying the contents of Ethernet packets

The `ether-display` command displays the hexadecimal contents of Ethernet packets being received and transmitted on an Ethernet port. You must specify how many octets of each packet you want to display.

The following example displays 12 octets of each packet on the Ethernet port (port 0):

```
admin> ether-display 0 12
Diagnostic output enabled

admin> ether-display 0 12
ETHER XMIT: 12 of 60 octets
107E1350: 00 c0 80 89 03 d7 00 c0 7b 6b 9f d6 ........
{k..
ETHER XMIT: 12 of 64 octets
107E1350: 00 c0 80 89 03 d7 00 c0 7b 6b 9f d6 ........
{k..
ETHER RECV: 12 of 60 octets
107B8FD4: 00 c0 7b 6b 9f d6 00 c0 80 89 03 d7 ........
{k..
ETHER XMIT: 12 of 407 octets
107E1350: 00 c0 80 89 03 d7 00 c0 7b 6b 9f d6 ........
```

```
{k..
ETHER XMIT: 12 of 161 octets
107E1350: 00 c0 80 89 03 d7 00 c0 7b 6b 9f d6 ........
{k..
ETHER RECV: 12 of 60 octets
..
..
..
```

To stop displaying the Ethernet statistics, specify 0 (zero) octets or use the `debug off` command, as shown in the following examples:

```
admin> ether-display 0 0
```

```
admin> debug off
```

Displaying Ethernet statistics and error counters

The `ether-stats` command displays all statistics and error counters maintained by the Ethernet driver.

This command uses the syntax

```
ether-stats 0 n
```

where Zero (`0`) is the first Ethernet port for which to display statistics and `n` is the last. For example:

```
admin> ether-stats 0Scb= 50
InProg= a1a00f6c
CuStatus= 1 RuStatus= 4
Handshake 0
Tx good:     84
   Maxcollisions:  0
   Latecollisions:  0
   dma under:   0
   no carrier:  0
   collisions:  0
   TxNoBuffers:  0
   Totalcollisions:  0
Rx good:     18109
   CRC:      0
   Alignment:   0
   NoResources  0
   Overrun:     0
   CDT:         0
   RxShort:     0
   RxPhyEr:     0
   RxRestarts:  0
Tcbs=160 Rfds=480 RfdLowWat=48
RfdHead=a1acee30 RfdTail=a1ace7d0 RfdCount=480
```

Displaying information about IGMP

The `igmp` command displays multicast information about Internet Group Membership Protocol (IGMP) groups and clients, if the Stinger unit is enabled for IP multicast forwarding. For syntax information, see the *Stinger Reference*.

To display information about active multicast client group addresses and interfaces, use the `-group` option. For example:

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

The field descriptions are as follows:

Field	Indicates
`Hash`	Index to a hash table (displayed for debugging purposes only). N/A indicates that the Default route is not an entry in the hash table.
`Group address`	IP multicast address used for the group. An asterisk indicates the IP multicast address being monitored, meaning that members join this address by local application. The Default route is the MBONE interface (the interface on which the multicast router resides). If the Stinger unit finds can find no member in a group, it forwards multicast traffic for the group to the MBONE interface.
`Members`	ID of each member of each multicast group. The zero ID represents members on the same Ethernet interface as the Stinger unit. All other IDs go to members of each group as they inform the Stinger unit that they have joined the group. If a client is a member of more than one group to which the Stinger unit forwards multicast packets, it has more than one multicast ID. The interface labeled `Mbone` is the interface on which the multicast router resides.
`Expire time`	When this membership expires. The Stinger unit sends out IGMP queries every 60 seconds, so the expiration time is usually renewed. If the expiration time is reached, the Stinger unit removes the entry from the table. If the field contains periods, this membership never expires. A string of periods means that the default route never times out.

Field	Indicates
Counts	Number of packets forwarded to the client, the number of packets dropped due to lack of resources, and the state of the membership. The state is displayed for debugging purposes.

To list all active multicast clients, use the `client` argument. For example:

```
admin> igmp client
IGMP Clients
Client      Version  RecvCount  CLU      ALU
0(Mbone)    1        0          0        0
2           1        39         68       67
1           1        33310      65       65
```

The field descriptions are as follows:

Field	Indicates
Client	Interface ID on which the client resides. The value 0 (zero) represents the Ethernet. Other numbers are WAN interfaces, numbered according to when they became active. The interface labeled `Mbone` is the interface on which the multicast router resides.
Version	Version of IGMP being used.
RecvCount	Number of IGMP messages received on that interface.
CLU ALU	`CLU` is current line utilization, and `ALU` is average line utilization. Both indicate the percentage of bandwidth used across this interface. If bandwidth utilization is high, some IGMP packet types are not forwarded.

To display IGMP messages with IP header errors, use the `netstat -s igmp` command. The output of this command shows the the number of IGMP messages received with an IP header length of 24 bytes (that is, the IP option is present, but without IP Alert option required for IGMP V2 messages).

The following sample output shows 40 packets received with IP header errors:

```
admin> netstat -s igmp
igmp:
4067 packets received
3814 query packets received
9 leave packets received
40 hdr error packets received
Alert
292 packets transmitted
89 query packets sent
175 response packets sent
28 leave packets sent
```

Displaying WAN IP interface information

The following commands provide information about WAN IP interfaces.

Displaying packets on WAN IP interfaces

The `wandisplay` command displays all packets received from, or sent to any of the IP WAN interfaces. Because `wandisplay` output shows what the Stinger unit is receiving from and sending to a remote device, the information can be very helpful in resolving PPP negotiation problems. The syntax of the command is as follows:

`wandisplay` *`number-of-octets-to-display`*

If you enter the command while traffic through the Stinger unit is heavy, the resulting amount of output can make your search for information tedious. The screen might even display the message `----- data lost -----`, which means that not all the output can be displayed on the screen.

Depending on the types of information you need to gather, you might prefer to use the `wandisplay` command during a period of low throughput, or to use `wandsess`, `wanopen`, or `wannext` to focus the display.

The following is an example of `wandisplay` command output. Note that the bytes are displayed in hexadecimal format.

```
admin> wandisplay 24
Display the first 24 bytes of WAN messages

> RECV-272:: 1 octets @ 5E138F74
  [0000]: 0D
RECV-272:: 13 octets @ 5E13958C
  [0000]: 0A 41 63 63 65 70 74 3A 20 69 6D 61 67
XMIT-276:: 1011 octets @ 2E12D8A4
  [0000]: 7E 21 45 00 03 EE 54 2B 40 00 37 06 BA 09 CF 2B
  [0010]: 00 86 D0 93 91 90 1A 0A
```

Enter `wandisplay 0` to disable the logging of this information:

```
admin> wandisplay 0
WAN message display terminated
```

Displaying WAN data for a particular user

The `wandsess` command shows WAN data as it is received and transmitted for a particular user. The `wandsess` command is very similar to the `wandisplay` command, but when you use `wandsess`, the system displays only incoming and outgoing packets for a specific user. The system displays bytes in hexadecimal format

The `wandsess` command is particularly helpful on a Stinger unit with several simultaneous active connections. The command acts as a filter, allowing you to focus your troubleshooting.

You can use the `wandsess` command only with LIMs. For syntax information, see the *Stinger Reference*. To use the `wandsess` command, specify a session name, which is the name of a local `connection` profile or a RADIUS user profile and the maximum number of octets to display per packet. If you specify 0 (zero), the Stinger unit does not display any data.

You must first open a session with a LIM. The following sample commands open session with the module in slot 7 and activate the display of 7 octets of data per packet for the user `tim`:

```
admin> open 1 7
modem-1/7> wandsess tim
RECV-tim:300:: 1 octets @ 3E13403C
  [0000]: 7E 21 45 00 00 3E 15 00 00 00 20 7D 31 C2 D2
RECV-tim:300:: 15 octets @ 3E133A24
  [0000]: D0 7D B3 7D B1 B3 D0 7D B3 90 02 04 03 00 35
XMIT-tim:300:: 84 octets @ 3E12D28C
  [0000]: 7E 21 45 00 00 4E C4 63 00 00 1C 7D 31 17 5F D0
  [0010]: 93 90 02 D0 93 91 B3 00
```

Displaying WAN data during connection establishment for users

The `wanopening` command shows WAN data as it is received and transmitted during connection establishment for all users. The `wanopening` command is particularly helpful for troubleshooting connection problems in which users make the initial connection, but are disconnected within a few seconds. The output of `wanopening` is very similar to the output of `wandisplay`, but `wanopening` shows packets only until the connection has been completely negotiated.

To use the `wanopening` command, you must first open a session with a LIM. using the `open` command. Then, enter the `wanopening` command with the maximum number of octets to display per packet. If you specify 0 (zero), the Stinger unit does not log WAN data.

For example, the following sample commands open a session with a LIM and activate the display of WAN data received and transmitted during connection establishment:

```
admin> open 1 7

modem-1/7> wanopening
Display the first 24 bytes of WAN messages
RECV-272:: 1 octets @ 5E138F74
  [0000]: 0D
RECV-272:: 13 octets @ 5E13958C
  [0000]: 0A 41 63 63 65 70 74 3A 20 69 6D 61 67
XMIT-276:: 1011 octets @ 2E12D8A4
  [0000]: 7E 21 45 00 03 EE 54 2B 40 00 37 06 BA 09 CF 2B
  [0010]: 00 86 D0 93 91 90 1A 0A
```

Note that the bytes are displayed in hexadecimal format.

Monitoring OSPF routing

6

The `ospf` diagnostic-level commands display information related to OSPF routing, including the link state advertisements (LSAs); the routing table for border routers; and the OSPF areas, interfaces, statistics, and routing table. Use `ospf` plus its options to monitor OSPF routing.

Overview of the OSPF command

To display `ospf` command usage, enter the `ospf` command with no arguments. Following is a listing of valid options for the `ospf` command:

Option	Displays
`stats`	OSPF statistics. “Displaying general information about OSPF routing” on page 6-2.
`size`	Size of the OSPF routing table. See “Displaying the OSPF database” on page 6-4.
`database`	OSPF database summary. See “Displaying the OSPF database” on page 6-4.
`ext`	OSPF external autonomous system advertisements. See “Displaying OSPF external advertisements” on page 6-6.

Option	Displays
internal	OSPF internal routes. See "Displaying OSPF internal advertisements" on page 6-7.
lsdb [***area***]	OSPF link-state database summary for an area. If you do not specify the ***area*** option, the summary for the first configured area (or for the only defined area) is displayed. If you specify the an area, the unit displays a summary for the specified area. Specifying an area is meaningful if the unit is operating as an area border router (ABR). **Note** With the current release, a Stinger unit cannot operate as an ABR, so each Stinger unit's OSPF interface belongs to the same area. See "Displaying the OSPF link-state database" on page 6-7.
lsa ***area ls-type ls-id ls-orig***	Detailed information about OSPF LSAs. ■ ***area***—Area ID. ■ ***ls-type***—LSA type. Specify one of the following options for ***ls-type***: – **rtr**—Type 1 router-LSA that describes the collected states of the router's interfaces. – **net**—Type 2 network-LSA that describes the set of routers attached to the network. – **sum**—Types 3 and 4 routes to networks in remote areas, or autonomous system border routers (ASBRs). ■ ***ls-id***—Target address of the router. ■ ***ls-orig***—Address of the advertising router. See "Displaying OSPF LSAs" on page 6-9.
rtab	OSPF routing table. See "Displaying the OSPF routing table" on page 6-10.
routers	OSPF router information. See "Displaying information about OSPF routers" on page 6-11.
intf [***ip_addr***]	Information about one or more OSPF interfaces. See "Displaying OSPF interfaces" on page 6-12.
nbrs [***ip_addr***]	Information about one or more OSPF neighbors. See "Displaying OSPF neighbors" on page 6-14.
translators	Router IDs of not-so-stubby area (NSSA) border routers.

Displaying general information about OSPF routing

To display general information about OSPF, enter the OSPF command with the `stats` option. For example:

```
admin> ospf stats
```

```
OSPF version:   2

OSPF Router ID:          10.103.0.254
AS boundary capability:   Yes
Attached areas:           1       Estimated # ext. (5) routes: 65536
OSPF packets rcvd:        71788   OSPF packets rcvd w/errs:    19
Transit nodes allocated:  812     Transit nodes freed:         788
LS adv. allocated:        2870    LS adv. freed:               2827
Queue headers alloc:      64      Queue headers avail:         64
# Dijkstra runs:          10      Incremental summ. updates:   0
Incremental VL udates:    0       Buffer alloc failures:       0
Multicast pkts sent:      27343   Unicast pkts sent:           1154
LS adv. aged out:         0       LS adv. flushed:             507
Incremental ext.(5) updates: 1014  Incremental ext.(7) updates: 0

External (Type 5) LSA database -
Current state:                    Normal
Number of LSAs:                   43
Number of overflows:           0
```

The fields in the output contain the following information:

Field	Indicates
OSPF version	Version of the OSPF protocols running.
OSPF Router ID	IP address assigned to the Stinger unit, which is typically the address specified for the Ethernet interface.
AS boundary capability	Border router capability. This column displays yes if the Stinger unit functions as an ASBR or no if it does not function as an ASBR.
Attached areas	Number of areas to which this Stinger unit attaches.
Estimated # ext.(5) routes	Number of LSA routes external to the OSPF autonomous system that the Stinger unit can maintain before it goes into an overload state. These routes are known as AS-external (type 5) routes.
OSPF packets rcvd	Total number of OSPF packets received by the Stinger unit.
OSPF packets rcvd w/ errs	Total number of OSPF errored packets received by the Stinger unit.
Transit nodes allocated	Allocated transit nodes generated only by router LSAs (type 1) and network LSAs (type 2).
Transit nodes freed	Freed transit nodes generated only by router LSAs (type 1) and network LSAs (type 2).
LS adv. freed	Number of LSAs freed.
Queue headers alloc	Number of queue headers allocated. LSAs can reside in multiple queues. Queue headers are the elements of the queues that contain the pointer to the LSA.

Field	Indicates
Queue headers avail	Available memory for queue headers. To prevent memory fragmentation, the Stinger unit allocates memory in blocks. The Stinger unit allocates queue headers from the memory blocks. When the Stinger unit frees all queue headers from a specific memory block, the unit returns the block to the pool of available memory blocks.
# Dijkstra runs	Number of times that the Stinger unit has run the Dijkstra algorithm (short path computation).
Incremental summ. updates	Number of summary updates that the Stinger unit runs when small changes cause generation of summary LSAs (type 3) and summary router LSAs (type 4).
Incremental VL updates	Number of incremental virtual link updates that the Stinger unit performs.
Buffer alloc failures	Number of buffer allocation problems that the Stinger unit has detected and from which it has recovered.
Multicast pkts sent	Number of multicast packets sent by OSPF.
Unicast pkts sent	Number of unicast packets sent by OSPF.
LS adv. aged out	Number of LSAs that the Stinger unit has aged and removed from its tables.
LS adv. flushed	Number of LSAs that the Stinger unit has flushed.
Incremental ext.(5) updates	Number of incremental AS-external LSA (type 5) updates.
Incremental ext.(7) updates	Number of incremental NSSA LSA (type 7) updates.
Current state	State of AS-external LSA (type 5) database: Normal or Overload.
Number of LSAs	Number of LSAs in the AS-external LSA (type 5) LSA database.
Number of overflows	Number of AS-external (type 5) LSAs that exceeded the limit of the database.

Displaying the OSPF database

To display the entire OSPF database, enter the OSPF command with the `database` option. For example:

```
admin> ospf database
                        Router Link States (Area: 0.0.0.0)
Type LS ID              LS originator     Seqno     Age   Xsum
RTR  10.101.0.1         10.101.0.1      0x800002a1  746  0x8bd8
RTR  10.101.0.2         10.101.0.2      0x800002d6  539  0x0ea1
RTR  10.102.0.1         10.102.0.1      0x800002a3 2592  0x9bc1
RTR  10.103.0.204       10.103.0.204    0x800001ba 1173  0x725f
```

```
RTR  10.103.0.254       10.103.0.254    0x80000301  534  0x7066
RTR  10.104.0.1         10.104.0.1      0x800002ad  777  0xb98e
RTR  10.104.0.2         10.104.0.2      0x80000193 1258  0x265a
RTR  10.105.0.2         10.105.0.2      0x80000299  865  0x4295
RTR  10.105.0.3         10.105.0.3      0x800002e5 1057  0x4449
RTR  10.105.0.4         10.105.0.4      0x80000310 1585  0x5775
RTR  10.105.0.61        10.105.0.61     0x800002ae 1204  0xcf2e
RTR  10.105.0.200       10.105.0.200    0x80000263  213  0x4b25
RTR  10.123.0.8         10.123.0.8      0x80000401 1071  0xecf2
RTR  10.123.0.254       10.123.0.254    0x80000401 1175  0xad39
RTR  12.151.0.2         12.151.0.2      0x800006ee  825  0x0531
RTR  192.1.1.1          192.1.1.1       0x8000039b   18  0xb04b
RTR  210.210.210.1      210.210.210.1   0x800001aa  201  0x5338
               # advertisements:       17
               Checksum total:         0x7946c
                       Network Link States (Area: 0.0.0.0)
Type LS ID              LS originator     Seqno     Age   Xsum
NET  10.101.0.1         10.101.0.1      0x80000236  746  0x1d45
NET  10.102.0.1         10.102.0.1      0x80000235 2592  0x1f40
NET  10.104.0.2         10.104.0.2      0x80000179  830  0x67a8
NET  10.105.0.8         10.123.0.8      0x80000304 1071  0x0ccd
NET  10.123.0.6         12.151.0.2      0x8000023d  825  0x59ed
NET  100.103.100.204    10.103.0.204    0x80000029  252  0x8b34
               # advertisements:       6
               Checksum total:         0x1961b
                       External ASE5 Link States
Type LS ID              LS originator     Seqno     Age   Xsum
ASE5 10.103.1.0         10.103.0.204    0x8000004f 1726  0xd23f
ASE5 10.103.2.0         10.103.0.204    0x8000004f 1716  0xc749
ASE5 10.103.3.0         10.103.0.204    0x8000004f 1704  0xbc53
ASE5 10.103.4.0         10.103.0.204    0x8000004f 1692  0xb15d
ASE5 10.103.6.0         10.103.0.204    0x8000004f 1672  0x9b71
ASE5 10.103.7.0         10.103.0.204    0x8000004f 1666  0x907b
ASE5 10.103.8.0         10.103.0.204    0x8000004f 1641  0x8585
ASE5 10.107.0.0         10.103.0.254    0x80000104  250  0x1413
ASE5 10.113.0.0         10.103.0.254    0x80000121  250  0x0e76
ASE5 10.200.0.2         10.103.0.254    0x80000001  231  0xa823
ASE5 10.222.0.2         10.103.0.254    0x80000001  202  0x9f16
ASE5 11.0.0.0           10.103.0.254    0x80000027  250  0x49a6
ASE5 11.103.0.0         10.103.0.254    0x80000121  250  0xfc10
ASE5 14.240.0.0         10.103.0.204    0x800001a4  199  0x0926
ASE5 50.151.0.2         10.103.0.254    0x80000121  250  0xa90a
ASE5 101.103.0.0        10.103.0.254    0x80000121  250  0x664c
..
..
               # advertisements:       44
               Checksum total:         0x191d3a
```

The fields in the output contain the following information:

Field	Indicates
Type	Type of link as defined in RFC 2328, *OSPF Version 2*: ■ Type 1 (RTR) are router LSAs that describe the collected states of the router's interfaces. ■ Type 2 (NET) are network LSAs that describe the set of routers attached to the network. ■ Types 3 and 4 (SUM) describe routes to networks in remote areas or autonomous system border routers (ASBRs). ■ Type 5 (ASE5) are AS-external LSAs that describe routes to destinations external to the autonomous system. A default route for the autonomous system can also be described by an AS-external-LSA. Use `ospf ext` to display only type 5 LSAs. ■ Type 7 (ASE7) are link advertisements that are only flooded within an NSSA.
LS ID	Target address of the route.
LS originator	Address of the advertising router.
Seqno	Hexadecimal number that begins with 80000000 and increments by one for each LSA received.
Age	Age of the route in seconds.
Xsum	Checksum of the LSA.
# advertisements	Total number of entries in the database.
Checksum total	Checksum of the database.

Displaying OSPF external advertisements

To display only OSPF AS-external (type 5) LSAs, advertisements, include the `ext` option with the `ospf` command. For example:

```
admin> ospf ext
Type LS ID              LS originator     Seqno     Age   Xsum
ASE5 10.103.1.0         10.103.0.204    0x8000004f 1702  0xd23f
ASE5 10.103.2.0         10.103.0.204    0x8000004f 1692  0xc749
ASE5 10.103.3.0         10.103.0.204    0x8000004f 1680  0xbc53
ASE5 10.103.4.0         10.103.0.204    0x8000004f 1668  0xb15d
ASE5 10.103.6.0         10.103.0.204    0x8000004f 1648  0x9b71
ASE5 10.103.7.0         10.103.0.204    0x8000004f 1642  0x907b
ASE5 10.103.8.0         10.103.0.204    0x8000004f 1617  0x8585
..
..
ASE5 214.240.0.127      10.103.0.204    0x800001a4  175  0xdb0b
ASE5 223.57.40.0        10.103.0.254    0x80000121  226  0x7540
ASE5 223.57.40.244      10.103.0.254    0x80000121  226  0xe3dc
               # advertisements:       46
               Checksum total:         0x1a1d9e
```

The output of this command is the same as for the `ospf database` command, with the exception of the type. The `ospf ext` command shows only type 5 LSAs.

Displaying OSPF internal advertisements

To display OSPF internal LSAs, include the `internal` option with the `ospf` command. For example:

```
admin> ospf internal
                Area: 0.0.0.1
Destination     Mask            Cost
33.240.0.0      255.255.255.224  1
103.240.0.0     255.255.255.192  1
113.240.0.0     255.255.255.128  1
183.240.0.0     255.255.255.128  1
193.240.0.0     255.255.255.128  1
203.240.0.0     255.255.255.128  1
```

The fields in the output contain the following information:

Field	Indicates
`Area`	Area in which the router resides.
`Destination`	Route's target address. To send a packet to this address, the Stinger unit uses this route. If the target address appears more than once in the routing table, the Stinger unit uses the most specific route (having the largest subnet mask) that matches that address.
`Mask`	Subnet mask of the route.
`Cost`	Cost of the router.

Displaying the OSPF link-state database

To display the link-state database for the first configured area (or for the only defined area), include the `lsdb` option with the `ospf` command. The Stinger unit does not currently operate as an ABR, so each Stinger unit's OSPF interface belongs to the same area. (That area number does not have to be the default backbone area 0.0.0.0.) For example:

```
admin> ospf lsdb
                        Area: 0.0.0.0
Type LS ID              LS originator     Seqno     Age   Xsum
RTR  10.101.0.1         10.101.0.1      0x8000029f  720  0x8fd6
RTR  10.101.0.2         10.101.0.2      0x800002d1  126  0x189c
RTR  10.102.0.1         10.102.0.1      0x800002a2  767  0x9dc0
RTR  10.102.0.2         10.102.0.2      0x800002cc  124  0x862c
RTR  10.103.0.204       10.103.0.204    0x800001b8 1147  0x765d
RTR  10.103.0.254       10.103.0.254    0x800002fb  167  0x8cc9
RTR  10.104.0.1         10.104.0.1      0x800002ab  751  0xbd8c
RTR  10.104.0.2         10.104.0.2      0x80000191 1232  0x2a58
RTR  10.105.0.2         10.105.0.2      0x80000297  843  0x4693
```

```
RTR  10.105.0.3         10.105.0.3      0x800002e3 1032  0x4847
RTR  10.105.0.4         10.105.0.4      0x8000030e 1560  0x5b73
RTR  10.105.0.61        10.105.0.61     0x800002ac 1178  0xd32c
RTR  10.105.0.200       10.105.0.200    0x80000261  194  0x4f23
RTR  10.123.0.8         10.123.0.8      0x800003ff 1045  0xf1ef
RTR  10.123.0.254       10.123.0.254    0x800003ff 1149  0xb236
RTR  12.151.0.2         12.151.0.2      0x800006ec  799  0x092f
RTR  192.1.1.1          192.1.1.1       0x80000398 1791  0xb648
RTR  210.210.210.1      210.210.210.1   0x800001a8  175  0x5736
NET  10.101.0.1         10.101.0.1      0x80000234  720  0x2143
NET  10.102.0.1         10.102.0.1      0x80000234  767  0x213f
NET  10.104.0.2         10.104.0.2      0x80000177  804  0x6ba6
NET  10.105.0.8         10.123.0.8      0x80000302 1045  0x10cb
NET  10.123.0.6         12.151.0.2      0x8000023b  799  0x5deb
NET  100.103.100.204    10.103.0.204    0x80000027  226  0x8f32
               # advertisements:       24
               Checksum total:         0xa2ae6
```

The fields in the output contain the following information:

Field	Indicates
`Area`	Area ID.
`Type`	Type of link as defined in RFC 2328: ■ RTR are Type 1 router-LSAs that describe the collected states of the router's interfaces. ■ NET are Type 2 network-LSAs that describe the set of routers attached to the network. ■ SUM are Types 3 and 4 LSAs that describe routes to networks in remote areas or autonomous system border routers (ASBRs). ■ ASE7 are Type 7 LSAs that are only flooded within an NSSA.
`LS ID`	Target address of the route.
`LS originator`	Address of the advertising router.
`Seqno`	Hexadecimal number that begins with 80000000 and increments by one for each LSA received.
`Age`	Age of the route in seconds.
`Xsum`	Checksum of the LSA.
`#advertisements`	Total number of entries in the link-state database.
`Checksum total`	Checksum of the link-state database.

You can expand each entry in the link-state database to view additional information about a particular LSA, as explained in the next section.

Displaying OSPF LSAs

To view detailed information about a link state advertisement (LSA), use the following syntax for the `ospf` command:

`ospf lsa` ***`area ls-type ls-id ls-orig`***

The command requires that you include the first four fields of the LSA as listed in the database. You can select the first four fields and paste them in after typing the command.

The following sample command shows an expanded view of an LSA from a Stinger unit in area 0.0.0.0 for an external route to the target address 10.5.2.160 from a router at 10.5.2.162:

```
admin> ospf lsa 0.0.0.0 ase 10.5.2.160 10.5.2.162
LSA  type: ASE ls id: 10.5.2.160 adv rtr: 110.5.2.162 age: 568
          seq #: 80000037 cksum: 0xfffa
          Net mask: 255.255.255.255 Tos 0 metric: 10 E type: 1
          Forwarding Address: 0.0.0.0 Tag: c0000000
```

The output differs depending on the type of link. The following is an example of a router LSA:

```
admin> ospf lsa 0.0.0.0 rtr 192.1.1.1 192.1.1.1
        LS age:      66
        LS options:  (0x2) E
        LS type:     1
        LS ID (destination): 192.1.1.1
        LS originator:       192.1.1.1
        LS sequence no:      0x80000399
        LS checksum:         0xb449
        LS length:           48
        Router type:     (0x2) ASBR
        # router ifcs:   2
                Link ID:          10.105.0.8
                Link Data:        10.105.0.7
                Interface type:   (2) TrnsNetwork
                        No. of metrics: 0
                        TOS 0 metric:   10 (0)
                Link ID:          10.123.0.6
                Link Data:        10.123.0.7
                Interface type:   (2) TrnsNetwork
                        No. of metrics: 0
                        TOS 0 metric:   10 (0)
```

The next example is for a network LSA:

```
admin> ospf lsa 0.0.0.0 net 100.103.100.204 10.103.0.204
        LS age:      814
        LS options:  (0x2) E
        LS type:     2
        LS ID (destination): 100.103.100.204
        LS originator:       10.103.0.204
        LS sequence no:      0x80000027
```

```
LS checksum:          0x8f32
LS length:            36
Network mask:         255.255.0.0
        Attached Router: 10.103.0.204     (1)
        Attached Router: 10.103.0.254     (1)
        Attached Router: 10.123.0.254     (1)
```

For information about the fields in the output of these commands, see RFC 2328.

Displaying the OSPF routing table

To display the OSPF routing table, include the `rtab` option with the `ospf` command. For example:

```
admin> ospf rtab
DTyp RType Destination       Area          Cost  Flags  Next hop(s)  IfNum
RTE  FIX   50.151.0.2/32      -               1     0x81   0.0.0.6         6
RTE  FIX   130.57.40.243/32   -              10     0x1    0.0.0.6         6
RTE  FIX   130.57.0.0/16      -              10     0x2    0.0.0.6         6
RTE  FIX   140.57.40.244/32   -              10     0x1    0.0.0.6         6
RTE  FIX   140.57.0.0/16      -              10     0x2    0.0.0.6         6
RTE  FIX   150.57.40.245/32   -              10     0x1    0.0.0.6         6
RTE  FIX   150.57.0.0/16      -              10     0x2    0.0.0.6         6
RTE  FIX   160.57.40.246/32   -              10     0x1    0.0.0.6         6
RTE  FIX   160.57.0.0/16      -              10     0x2    0.0.0.6         6
..
```

The fields in the preceding output contain the following information:

Field	Indicates
`DType`	Internal route type. DType displays one of the following values: RTE (generic route), ASBR (autonomous system border route), or BR (area border route).
`RType`	Internal router type. RType displays one of the following values: FIX (static route), NONE, DEL (deleted or invalid state), OSPF (OSPF-computed), OSE1 (type 1 external), or OSE2 (type 2 external).
`Destination`	Destination address and subnet mask of the route.
`Area`	Area ID of the route.
`Cost`	Cost of the route.
`Flags`	Hexadecimal number representing an internal flag.
`Next hop(s)`	Next hop in the route to the destination.
`IfNum`	Number of the interface used to reach the destination.

Displaying information about OSPF areas

To display information about OSPF areas, include the `areas` option with the OSPF command. For example:

```
admin> ospf areas
Area ID  Authentication  Area Type #ifcs  #nets  #rtrs  #brdrs  #intnr
0.0.0.0  Simple-passwd   Normal      1      0      2       0       3
```

The fields in the output contain the following information:

Field	Indicates
`Area ID`	Area number in dotted-decimal format.
`Authentication`	Type of authentication: simple password, MD5, or null.
`Area Type`	Type of OSPF area: normal, stub, or NSSA.
`#ifcs`	Number of Stinger unit interfaces specified in the area.
`#nets`	Number of reachable networks in the area.
`#rtrs`	Number of reachable routers in the area.
`#brdrs`	Number of reachable area border routers (ABRs) in the area.
`#intnr`	Number of reachable internal routers in the area.

Displaying information about OSPF routers

To display OSPF routers, include the `routers` option with the OSPF command. For example:

```
admin> ospf routers
DType RType Destination   Area         Cost     Next hop(s)     IfNum
ASBR  OSPF  10.101.0.1    0.0.0.0        11    10.101.0.2       20
ASBR  OSPF  10.101.0.2    0.0.0.0        10    10.101.0.2       20
ASBR  OSPF  10.103.0.204  0.0.0.0        1     100.103.100.204  24
ASBR  OSPF  10.104.0.1    0.0.0.0        12    10.105.0.4       21
                                              10.105.0.61      21
ASBR  OSPF  10.104.0.2    0.0.0.0        11    10.105.0.4       21
                                              10.105.0.61      21
  BR  OSPF  10.105.0.2    0.0.0.0        1     10.105.0.2       21
ASBR  OSPF  10.105.0.2    0.0.0.0        1     10.105.0.2       21
ASBR  OSPF  10.105.0.3    0.0.0.0        1     10.105.0.3       21
ASBR  OSPF  10.105.0.4    0.0.0.0        1     10.105.0.4       21
ASBR  OSPF  10.105.0.61   0.0.0.0        1     10.105.0.61      21
ASBR  OSPF  10.105.0.200  0.0.0.0        1     10.105.0.200     21
ASBR  OSPF  10.123.0.8    0.0.0.0        1     10.105.0.8       21
ASBR  OSPF  10.123.0.254  0.0.0.0        1     100.103.100.123  24
  BR  OSPF  12.151.0.2    0.0.0.0        1     10.105.0.6       21
ASBR  OSPF  192.1.1.1     0.0.0.0        1     10.105.0.7       21
```

The fields in the output contain the following information:

Field	Specifies
DType	Internal route type. DType displays one of the following values: RTE (generic route), ASBR (AS border route), or BR (area border route).
RType	Internal router type.
Destination	Router's IP address.
Area	Area in which the router resides.
Cost	Cost of the router.
Next hop(s)	Next hop in the route to the destination.
IfNum	Number of the interface used to reach the destination.

Displaying OSPF interfaces

To display summarized information about all OSPF interfaces or specific information about a single interface, include the `intf` option with the `ospf` command.

Displaying summarized information

To display summarized information on OSPF interfaces, enter the following command:

```
admin> ospf intf
Ifc Address     Phys     Assoc. Area Type   State    #nbrs #adjs  DInt
10.103.0.254    ie0      0.0.0.0     Brdcst DR        0     0      40
10.105.0.254    ie1-7-1  0.0.0.0     Brdcst Other     9     1      40
100.103.100.254 ie1-7-4  0.0.0.0     Brdcst Other     2     2      40
50.151.0.2      apx1     0.0.0.0     P-P    P-P       0     0      120
10.103.0.254    m2       0.0.0.0     P-P    P-P       1     1      120
10.103.0.254    m1       0.0.0.0     P-P    P-P       1     1      120
```

The fields in the output contain the following information:

Field	Setting
Ifc Address	Address assigned to the Stinger unit's Ethernet interface. To identify WAN links, use the `Type` and `Cost` fields.
Phys	Name of the interface or the `connection` profile for WAN links.
Assoc. Area	Area in which the interface resides.
Type	Point-to-point (P-P) or Broadcast (Brdcst). WAN links are point-to-point links.
State	State of the link according to RFC 2328. There are many possible states, and not all states apply to all interfaces.
#nbrs	Number of neighbors of the interface.

Field	Setting
#adjs	Number of adjacencies on the interface.
DInt	Number of seconds that the Stinger unit waits for a router update before removing the router's entry from its table. The interval is called the *dead* interval.

Displaying information about a specific interface

To display detailed information for a specific interface, enter the `ospf` command with the `intf` option along with the interface IP address in dotted decimal notation. For example:

```
admin> ospf intf 194.194.194.2
              Interface address:      194.194.194.2
              Attached area:          0.0.0.0
              Physical interface:     phani (wan1)
              Interface mask:         255.255.255.255
              Interface type:         P-P

             State:                  (0x8) P-P
              Designated Router:      0.0.0.0
              Backup DR:              0.0.0.0
              Remote Address:         194.194.194.3
DR Priority:       5  Hello interval:  30   Rxmt interval:  5
Dead interval:   120  TX delay:         1   Poll interval:  0
Max pkt size:   1500  TOS 0 cost:      10
# Neighbors:       1  # Adjacencies:    1   # Full adjs.:   1
# Mcast floods: 1856  # Mcast acks:  1855
```

The fields in the output contain the following information:

Field	Setting
Interface Address	IP address specified for the Stinger unit's Ethernet interface.
Attached Area	Area in which the interface resides.
Physical interface	Name of the interface or the Connection profile for WAN links.
Interface mask	Subnet mask for the interface.
Interface type	Point-to-point (P-P) or broadcast (Bcast). WAN links are point-to-point links.
State	State of the link according to RFC 2328. There are many possible states, and not all states apply to all interfaces.
Designated Router	IP address of the designated router for the interface.
Backup DR	IP address of the backup designated router (BDR) for the interface.

Field	Setting
Remote Address	IP address of the remote end of a point-to-point (WAN) link.
DR Priority	Priority of the designated router.
Hello interval	Interval in seconds that the Stinger unit sends Hello packets (as defined in RFC 2328).
Rxmt interval	Retransmission interval (as described in RFC 2328).
Dead interval	Number of seconds that the Stinger unit waits for a router update before removing the router's entry from its table.
TX delay	Interface transmission delay.
Poll interval	Poll interval of nonbroadcast multiaccess (NBMA) networks.
Max pkt size	Maximum size of a packet that the Stinger unit can send to the interface.
TOS 0 cost	Type of service normal (*0*) cost.
# Neighbors	Number of neighbors.
# Adjacencies	Number of adjacencies.
# Full adjs.	Number of fully formed adjacencies.
# Mcast floods	Number of multicast floods on the interface.
# Mcast acks	Number of multicast acknowledgments on the interface.

Displaying OSPF neighbors

To display information about OSPF neighbors to the Stinger unit, include the `nbrs` option with the OSPF command. For example:

```
admin> ospf nbrs

Neighbor ID    Neighbor addr     State       LSrxl  DBsum  LSreq  Ifc  Prio
10.105.0.4     10.105.0.4        2Way/-      0      0      0      5    ie1-7-1
10.105.0.2     10.105.0.2        2Way/-      0      0      0      5    ie1-7-1
12.151.0.2     10.105.0.6        2Way/-      0      0      0      1    ie1-7-1
10.105.0.3     10.105.0.3        2Way/-      0      0      0      5    ie1-7-1
10.105.0.61    10.105.0.61       2Way/-      0      0      0      5    ie1-7-1
210.210.210.1  10.105.0.49       Exstar/BDR  0      0      0      5    ie1-7-1
192.1.1.1      10.105.0.7        2Way/-      0      0      0      5    ie1-7-1
10.123.0.8     10.105.0.8        Full/DR     0      0      0      5    ie1-7-1
10.105.0.200   10.105.0.200      2Way/-      0      0      0      5    ie1-7-1
```

```
10.103.0.204    100.103.100.204    Full/DR     0     0     0     5   ie1-7-4
10.123.0.254    100.103.100.123    Full/BDR          0     0     5   ie1-7-4
10.102.0.2      10.102.0.2         Init/-      00    0     0     5   m1
10.101.0.2      10.101.0.2         Full/-      0     0     0     5   m1
```

The fields in the output contain the following information:

Field	Setting
`Neighbor ID`	Address assigned to the interface. In the Stinger unit, the IP address is always the address assigned to the Ethernet interface.
`Neighbor addr`	IP address of the router used to reach a neighbor (often the same address as the neighbor itself).
`State`	State of the link-state database exchange. `Full` indicates that the databases are fully aligned between the Stinger unit and its neighbor. For a description of possible states, see RFC 2328.
`LSrxl`	Number of LSAs in the retransmission list.
`DBsum`	Number of LSAs in the database summary list.
`LSreq`	Number of LSAs in the request list.
`Ifc`	Interface name for the `ethernet` or `connection` profile name for the WAN.
`Prio`	Designated router election priority assigned to the Stinger unit.

To display information about a particular OSPF neighbor, append the `neighbor id` value to the `nbrs` option. For example:

```
admin> ospf nbrs 10.105.0.4
OSPF Router ID:         10.105.0.4
               Neighbor IP address:    10.105.0.4
               Neighbor State:         (0x8) 2Way
               Physical interface:     ie1-7-1 (ie1-7-1)
               DR choice:              10.105.0.8
               Backup choice:          10.105.0.49
               DR Priority:            5
  DB summ qlen:      0  LS rxmt qlen:      0  LS req qlen:       0
  Last hello:        6
  # LS rxmits:       0  # Direct acks:     0  # Dup LS rcvd:     0
  # Old LS rcvd:     0  # Dup acks rcv:    0  # Nbr losses:      0
  # Adj. resets:     0
```

Monitoring ATM and PNNI

7

The Stinger unit supports network management profiles and commands that are useful for locating the sources of problems on the network and for communicating with other hosts for management purposes. The following sections describe the commands and profiles that you use to monitor Asynchronous Transfer Mode (ATM) and Private Network-to-Network Interface (PNNI) operations.

For more information about the commands described in this chapter, see the *Stinger Reference*.

Monitoring ATM networks

Table 7-1 lists the profiles and commands that you use for monitoring ATM operations. For information about configuring a Stinger unit for ATM operations, see the *Stinger ATM Configuration Guide*.

Table 7-1. Profiles and commands for monitoring ATM networks

Profile or command	Used for
`atmvccstat` command	"Using the ATM status window" on page 7-2
`atm-internal-stat: line-state` parameter	"Determining ATM line status" on page 7-3
`atminternallines` command	"Displays the status of ATM internal lines" on page 7-4
`atmtrunkmgr` command	
`atmvcc-stat` profile	"Checking the status of a VCC interface" on page 7-5
`atmvcc-stat` profile `atmpvc-stat` profile	"Checking the status of a terminating PVC" on page 7-6

Table 7-1. Profiles and commands for monitoring ATM networks (Continued)

Profile or command	Used for
`atmvccmgr` command	"Displaying ATM VCC information and packet statistics" on page 7-6
`atmvcl` command `atmvpl` command	"Displaying ATM virtual link information" on page 7-7
`atmvcx` command `atmvpx` command	"Displaying ATM virtual link cross-connect information" on page 7-10
`spvcc` command	"Displaying SPVC information" on page 7-11
`atm-spvc-addr-config:spvc -atm-address` parameter `spvcshow` command	"Displaying SPVC target ATM addresses" on page 7-13
`spvcstat` command	"Monitoring failing SPVCs" on page 7-14
`atmsig` command	"Displaying signal statistics" on page 7-14
`atmcacstat` command	"Displaying CAC bandwidth allocation statistics" on page 7-15
`atmqos` command	"Displaying QoS statistics" on page 7-18
`atmconnectionfailures` command	"Displaying ATM connection failures" on page 7-18

Using the ATM status window

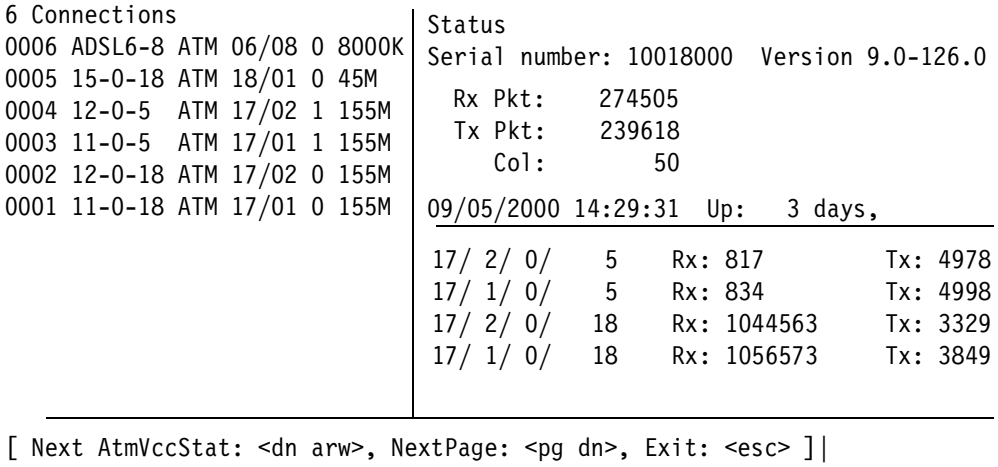
The `atmvccstat` command displays an 80-column by 24-row VT100 status window of active virtual channel connections (VCCs). This window behaves similarly to other status windows supported in the Stinger unit, as described in "Using the status window" on page 1-37.

To open the window, enter the `atmvccstat` command as follows:

```
admin> atmvccstat
```

When the window opens, the system prompt moves to just below the status window as shown in Figure 7-1.

Figure 7-1. Status window for ATM VCCs



By default, the left area of the window displays connection information. One line appears for each active connection, showing the user or station name, type of connection, physical address within the Stinger system (*shelf/line/channel*) on which the call is established, and the bandwidth of the connection. You can use the Pg Up and Pg Dn keys to display additional information if more connections are active than can be displayed in one screen.

The top right area of the window displays general status information about the Stinger unit, including its serial number, the version of system software that is running, and the number of cells transmitted and received. This area also shows the current system date and time and how long the system has been running since its most recent restart.

The bottom right area of the window displays information about active lines in the format *slot/port/virtual path identifier (VPI)/virtual channel identifier (VCI)*, and the number of cells transmitted and received.

For details about customizing the type of information that is displayed in the three areas of the window, see the "Customizing the status window display" on page 1-40.

To close the status window, enter the `status` command. (If the system prompt is not visible below the status window, press Escape to display it.)

```
admin> status
```

Determining ATM line status

To determine whether an ATM connection is active, use the `get` command to display the setting of the `line-state` parameter in the `atm-internal-stat` profile for that line. The ATM connection is active if the value for this parameter is `active`. For example:

```
admin> get atm-internal-stat {1 13 1} line-state
ATM-INTERNAL-STAT/{ shelf-1 slot-13 1 }
line-state = active
```

Displays the status of ATM internal lines

The `atminternallines` command displays the status of ATM lines. For command options, see the *Stinger Reference*. To display statistics for all ATM lines, use the `atminternallines -a` command. For example:

```
admin> atminternallines -a
All ATM Internal lines:
                                (dvOp   dvUpSt  dvRq    sAdm    nailg)
  Line    {    1  2  1 }        (Up      Assign  UP      UP     00051)
  Line    {    1  9  1 }        (Up      Assign  UP      UP     02449)
```

The data displayed includes the physical address of each line and the following information:

Field	Indicates
`dvOp`	Current operational state of the line. `Down` indicates that the line is in a nonoperational state. `Up` indicates that the line is in normal operations mode.
`dvUpSt`	Status of the line in normal operations mode. `Idle` indicates that no call is on the line. `Active` indicates that the line is handling a call.
`dvRq`	Required state of the line. `Down` indicates that the line is required to be nonoperational.`Up` indicates that the line is required to be in normal mode.
`sAdm`	Desired administrative state of the line. `Down` specifies that the line should terminate all operations and enter the down state. `Up` specifies that the line should start up in normal operations mode. Actual state of the line can differ from the desired state, as when a device is powering up or you change the desired state on a running slot. Changing the desired state does not automatically change a line to the desired state. It indicates that an operation has been initiated to change the Stinger unit to the state desired.
`nailg`	Dedicated (nailed) group to which the line is assigned.

Changing ATM debug levels

The `atmtrunkmgr -t` command toggles the debug level from 0 through 4. Each entry of the `atmtrunkmgr -t` command adds 1 to the debug level. After level 4 is reached, the level is reset to 0. The following sample commands change the debug level from 1 to 2:

```
admin> atmtrunkmgr -t
current atmtrunkmgr debug level = 1
admin> atmtrunkmgr -t
current atmtrunkmgr debug level = 2
```

Displaying the status of ATM trunk modules and their connections

The `atmtrunkmgr -g` *`connection-profile-name nailed-group`* display status of dedicated (nailed) groups.

If the code is 1, there is an active nailed group to connect to. If the interface is not operational, the return code is 0 (zero).

The following example queries a connection named ckt with nailed group 801:

```
admin> atmtrunkmgr -g ckt 801
return from atmTrunkDevGetChansByNGAndProf chan= 1.
```

Checking the status of a VCC interface

The system creates an `atmvcc-stat` profile for each virtual channel connection (VCC) interface. These profiles provide status information about each side of a circuit. You can read these profiles to check VCC status. Following are the relevant parameters, shown with sample settings:

```
[in ATMVCC-STAT/{ shelf-1 slot-10 47 0 35 }]
vcc-ident* = { shelf-1 slot-10 47 0 35 }
circuit-name = kam-1
current-state = vcc-data-transfer
vcc-type = connecting
```

Parameter	Setting
`vcc-ident`	Unique VCC identifer, made up of the interface address (shelf, slot, and modem numbers), the VPI, and the VCI.
`circuit-name`	Name of the permanent virtual circuit (PVC), which is the value of the `station` parameter in a local profile or the User-Name attribute in a RADIUS profile.
`current-state`	Current state of the circuit. The value of this parameter can be `vcc-inactive`, `vcc-closed` (the VCC exists but is closed), or `vcc-data-transfer` (the VCC is operational and data can be transferred).
`vcc-type`	For an ATM circuit, the value of this parameter is always `connecting` (point-to-point connecting). The other possible value is `terminating`. (For details, see the *Stinger ATM Configuration Guide*.)

The system also creates an `atmpvc-stat` profile for each configured ATM circuit. Following are the relevant parameters, shown with sample settings:

```
[in ATMPVC-STAT/kam-1]
circuit-name* = kam-1
pvc-type = connecting
```

```
current-state = pvc-data-transfer
vcc-members = [ { shelf-1 slot-10 47 0 35 } { shelf-1 slot-2 1 0 77 } ]
```

Parameter	Setting
`circuit-name`	Name of the PVC, which is the value of the `station` parameter in a local profile or the User-Name attribute in a RADIUS profile.
`pvc-type`	For an ATM circuit, the value of this parameter is always `connecting` (point-to-point connecting). The other possible value is `terminating` (see "Checking the status of a terminating PVC" on page 7-6).
`current-state`	Current state of the circuit. The value of this parameter can be `pvc-inactive`, `pvc-closed` (the PVC exists but is closed), or `pvc-data-transfer` (the PVC is operational and data can be transferred).
`vcc-members`	Both member VCCs of the circuit (the two sides). Each side has a unique VCC identifer, made up of the interface address (shelf, slot, and modem numbers), the VPI, and the VCI.

Checking the status of a terminating PVC

For terminating PVCs, the values in the `atmvcc-stat` and `atmpvc-stat` profiles are slightly different for terminating connections. Following are the relevant parameters (shown with sample settings):

```
[in ATMVCC-STAT/{ shelf-1 slot-17 1 0 35 }]
vcc-ident* = { shelf-1 slot-17 1 0 35 }
circuit-name = dsltnt-1
current-state = vcc-data-transfer
vcc-type = terminating
```

```
[in ATMPVC-STAT/dsltnt-1]
circuit-name* = dsltnt-1
pvc-type = terminating
current-state = pvc-data-transfer
vcc-members = [ { shelf-1 slot-17 1 0 35 }]
```

For terminating connections, the value of the `vcc-type` and `pvc-type` parameters is always `terminating`, and `vcc-members` always specifies a single member. The rest of the parameters in the profiles are the same for terminating PVCs as for ATM circuits. For details, see "Checking the status of a VCC interface" on page 7-5.

Displaying ATM VCC information and packet statistics

To display overall ATM virtual channel connection (VCC) information and packet statistics for a particular slot on a Stinger unit, use the `atmvccmgr` debug command. For the system to respond to this command, your `user` profile must be enabled with

debug privileges. For information on enabling debug privileges see "Enabling debug permissions" on page A-1.

Note You cannot enter the `atmvccmgr` command from the secondary control module.

To display status information for all ATM connections, use the `-a` option:

```
admin> atmvccmgr -a
```

Profile	Type	RouteId	ifnum	This Slot/Port/VPI/VCI	Other Slot/Port/VPI/VCI
adtran2/09	CONN.	0	0	17/1/0/15	64/1/0/39

Trunk module statistics are reported from the control module. The following sample command displays statistics for a trunk module in slot 17, port 1, VPI 0, and VCI 33:

```
admin> atmvcc -r 17 1 0 33
```

Received Cells	Discarded Cells	RX packets	Discarded packets	Error packets	Cells in last Pkt
0	0	0	0	0	392

For line interface module (LIM) statistics, you must first open a session with that module. The following sample commands display statistics for slot 14:

```
admin> auth super
super> open 1 14
sdsl-atm-v2-1/14> atmvccm -r 14
               Received   *Discarded Tagged    PCR Non-conform
port/vpi/vci   Cells      Cells      Cells     Cell count
  1/  0/   35  0          0          0         0
  2/  0/   35  9184       8163       0         7144
  3/  0/   35  0          0          0         0
  5/ 10/   35  0          0          0         0
  7/  0/   50  0          0          0         0
* Note: The Discarded Cells count includes the total
        number of cells dropped due to GCRA non conformance
        plus cells discarded due to partial packet discard
        (if PPD is enabled).
```

Displaying ATM virtual link information

An ATM connection between two devices is a virtual link. A virtual link can be a virtual channel link (VCL) or virtual path link (VPL), depending on whether it is identified by a VPI-VCI pair or the VPI field alone. For more details, see the *Stinger ATM Configuration Guide*.

To display VCL information, use the `atmvcl` command. For information about VPLs, use the `atmvpl` command. To display usage information, enter the command without any arguments or see the *Stinger Reference*.

With the `-a` option, both commands display information about all configured ATM VCLs or VPLs and their status. The `-s` and `-p` options enable you to display the same information as the `-a` option, but to restrict the output to links on a specific slot or slot-port combination. For example, the following sample command displays information about the VCLs for port 1 in slot 18:

```
admin> atmvcl -p 18 1
 Intf Slot  Port   Vpi    Vci    XConnID  Kind  OStatus
   15   18     1     0   1000          2   pvc       up
   15   18     1     0   1001          3   pvc       up
   15   18     1     0   1002          9   pvc       up
   15   18     1     0   1003          4   pvc       up
   15   18     1     0   1004          5   pvc       up
```

The `atmvpl` command produces similar output, except it does not include a VCI field. For example:

```
admin> atmvpl -p 18 1
 Intf Slot  Port  Vpi   XConnID  Kind  OStatus
   16   18     1   10         7   pvc       up
   16   18     1   20         1   pvc       up
...
```

In the preceding examples, the fields report the following information.

Field	Indicates
`Intf`	ATM interface index.
`Slot`	Slot number in the Stinger unit.
`Port`	Port number on the specified slot.
`Vpi`	VPI assigned to the link.
`Vci`	VCI assigned to the link (`atmvcl` command only).
`XConnID`	Cross-connect ID, which indicates whether the link is cross-connected to another link to form an ATM circuit.
`Kind`	Call control type.
`OStatus`	Current operational status of the link (`up` or `down`).

With the `-d` option, the command displays additional details about a specific VCL, identified by the slot, port, and VPI-VCI pair. The following sample command displays information about a VCL on slot 3, port 1, VPI 0, and VCI 41. The output indicates that this is a terminating connection using ATM adaptation layer 5 (AAL5):

```
admin> atmvcl -d 3 1 0 41
Physical Address = { 1 3 1 }
Interface = 65
VCC Endpoint = yes
Vpi = 0
Vci = 41
Oper Status = up
Rx Traffic Descr Index = 1
Tx Traffic Descr Index = 1
Conn Kind = pvc
```

```
Cast Type = p2p
AAL Type = aal5
AAL5 Rx SDU Size = 9188
AAL5 Tx SDU Size = 9188
AAL5 Encap Type  = llcEncapsulation
```

The following sample command shows information about a VPL on slot 18, port 1 that is cross-connected to another VPL in the system:

```
admin> atmvpl -d 18 1 20
Physical Address = { 1 18 2 }
Interface = 16
Vpi = 20
Oper Status = up
Rx Traffic Descr Index = 1
Tx Traffic Descr Index = 1
Conn Kind = pvc
Cast Type = p2p
Cross Connect ID = 1
```

The output of the preceding examples reports the following information:

Field	Indicates
Physical Address	Address of the physical interface in the Stinger unit.
Interface	ATM interface index.
VCC Endpoint	Whether the link terminates a virtual connection (yes or no).
Vpi	VPI assigned to the link.
Vci	VCI assigned to the link (atmvcl command only).
Oper Status	Current operational status of the link (up or down).
Rx Traffic Descr Index	Traffic descriptor index in the receive direction. A 1 (one) indicates the default traffic descriptor.
Tx Traffic Descr Index	Traffic descriptor index in the transmit direction. A 1 (one) indicates the default traffic descriptor.
Conn Kind	Call control type.
Cast Type	Connection topology type. The p2p value indicates point-to-point.
Cross Connect ID	A cross-connect ID. If present, this field indicates that the link is cross-connected to another link to form an ATM circuit. This field is not displayed for a terminating link.
AAL Type	ATM adaptation layer (AAL) type. This field is not displayed for a cross-connected link.
AAL5 Rx SDU Size	Receive source data unit (SDU) size of an AAL5 terminating link. This field is not displayed for a cross-connected link.
AAL5 Tx SDU Size	Transmit SDU size of an AAL5 terminating link. This field is not displayed for a cross-connected link.
AAL5 Encap Type	Type of encapsulation used for the AAL5 terminating link. This field is not displayed for a cross-connected link.

The following sample command shows VCL information for the Stinger unit. The output shows the number of terminating PVCs, PVC segments without cross-connections (created by SNMP), and PVC segments with cross-connections.

```
admin> atmvcl -c
Totals:              Up      Down
  PVC XConnect       1576     768
  PVC Terminate       152      48
  PVC Legs Only         0       4
  SVC In              591       0
  SVC Out             399       0
  SPVC Initiator      192       0
  SPVC Target         384       0
  Invalid               0
```

Displaying ATM virtual link cross-connect information

A cross-connect is a configuration in which the Stinger unit receives a cell stream on one interface and transmits it on another interface. Cross-connects are called ATM circuits in the Stinger command-line interface. For more details, see the *Stinger ATM Configuration Guide*.

To display information about virtual channel (VC)-switching ATM circuits, use the `atmvcx` command. For information about virtual path (VP)-switching ATM circuits, use the `atmvpx` command. For syntax information, see the *Stinger Reference*.

With no options on the command line, the commands display the usage statement. With the `-a` option, they display information about all configured virtual-channel-switching or virtual-path-switching circuits and their status. The `-s` and `-p` options enable you to display the same information as the -a option, but to restrict the output to links on a specific slot or slot-port combination. For example, the following command displays information about all virtual-circuit-switching cross-connects:

```
admin> atmvcx -a
```

		Low						High					
Profile	Kind	Intf/	Slot/	Port/	VPI/	VCI/	OStatus	Intf/	Slot/	Port/	VPI/	VCI/	Intf
lim-3-1	pvc	15	18	1	0	1000	up	65	3	1	0	41	up
lim-3-2	pvc	15	18	1	0	1001	up	66	3	2	0	41	up
lim-3-3	pvc	15	18	1	0	1002	up	67	3	3	0	41	up
lim-3-4	pvc	15	18	1	0	1003	up	68	3	4	0	41	up

Field	Indicates
Profile	Name of the profile in which the ATM circuit is configured.

Field	Indicates
Kind	Call control type.
Intf	ATM interface index.
Slot	Slot on which a VCL of the cross-connect is established. *Low* refers to the ATM interface that has a numerically lower interface index value than the other ATM interface identified in the cross-connect. *High* refers to the ATM interface with the numerically higher interface index value.
Port	Port of the specified slot on which a VCL of the cross-connect is established. *Low* refers to the ATM interface that has a numerically lower interface index value than the other ATM interface identified in the cross connect. *High* refers to the ATM interface with the numerically higher interface index value.
VPI	VPI assigned to the VCL.
VCI	VCI assigned to the VCL.
OStatus	Current operational status of the cross-connect.

Displaying SPVC information

The `spvcc` command displays information about soft PVC (SPVC) connections. To display information about SPVCs that use virtual-path switching (SPVPs), use the `spvpc` command. For syntax information, see the *Stinger Reference*.

With no options on the command line, the commands display the usage statement. With the `-a` option, they display information about all configured virtual-channel-switching or virtual-path-switching SPVCs and their status. The `-s` and `-p` options enable you to display the same information as the `-a` option, but to restrict the output to links on a specific slot or slot-port combination. For example, the following command displays information about all virtual-channel-switching SPVCs:

```
admin> spvcc -a

Profile      Intf  Slot/  Port  VPI  VCI  targVPI  targVCI  TargSel  TargSel
             /           /     /    /    /        /        /        /
spvc-init    16    18     2     5    100  7        100      req      inProg
```

The value displayed in the `OStatus` field indicates the current status of the SPVC connection. In the sample output, the field indicates that establishment of the connection is in progress. Once the connection is established, the status is `connected`.

With the `-d` option, each command displays additional details about a specific SPVC, identified by the slot, port, and VPI (or VPI-VCI pair). For example, the following command displays the details about an SPVC in slot 18, port 2, with VPI 5 and VCI 100:

```
admin> spvpc -d 18 2 5 100
Profile = spvc-init-1
Physical Address = { 1 18 2 }
```

```
Interface = 16
OperStatus = inProg
VCL Vpi = 5
TargetSelect = req
TargetVpi = 7
Target ATM address = 47.41.0.31.0.31.0.31.0.31.0.31.11.22.33.44.55.66.0.0.
LastReleaseCause = 3
LastReleaseDiagnostic = 81
RetryFailures = 10
RetryInterval = 10
RetryTimer = 5
RetryThreshold = 1
RetryLimit = 0
```

Field	Indicates
Profile	Name of the profile in which the SPVC or SPVPC is configured.
Physical Address	Address of the physical interface in the Stinger unit.
Interface	ATM interface index.
OperStatus	Current operational status of the SPVC.
VCL Vpi	VPI value of the initiating PVC.
TargetSelect	Method of assigning the VPI-VCI pair for the target PVC. The req value indicates that the initiating switch supplies the target VPI-VCI assignments during the signaling setup. The any value means the target switch provides the VPI-VCI pair.
TargetVpi	VPI value of the link used at the target PVC.
Target ATM address	Target ATM address of the SPVC.
LastReleaseCause	Value of the cause field of the cause information element in the last RELEASE message received for the SPVC. The value indicates the reason for the release.
LastReleaseDiagnostic	Value of the first 8 bytes of diagnostic information from the cause field of the cause information element in the last RELEASE message received for the SPVC.
RetryFailures	Number of attempts to establish the connection that have failed. This count is reset when the SPVC is established or restarted
RetryInterval	Number of seconds the system waits before attempting to establish the SPVC after the first failed call attempt.
RetryTimer	Current value of the retry timer for this connection. When the value reaches zero, the system attempts to establish the SPVC.
RetryThreshold	Number of consecutive call setup attempts that must fail before incrementing the atmSoftPvcCallFailures object, which can cause the system to generate an alarm.
RetryLimit	Maximum number of consecutive unsuccessful call setup attempts.

Displaying SPVC target ATM addresses

Each trunk port and LIM port that supports ATM has an associated ATM interface. In a Stinger unit enabled with the Lucent Technologies, Inc. Private Network-to-Network Interface (PNNI) license, the system assigns each ATM interface with a unique soft PVC (SPVC) target address. The address is used in the signaling required to establish both initiator and target SPVCs. The SPVC target address is defined in the Soft PVC MIB, and in the `atm-spvc-addr-config` profile.

You can view the ATM address assigned to an interface by displaying the value of the `spvc-atm-address` parameter. For example, the following command displays the address assigned to interface 1 of slot 3:

```
admin> get atm-spvc-addr-config { {1 3 1 } 0 } spvc-atm-address
[in ATM-SPVC-ADDR-CONFIG/{ { shelf-1 slot-3 1 } 0 }:spvc-atm-address]
spvc-atm-address = 39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:03:00:00:00:01:00
```

The `spvcshow` command displays SPVC target addresses and the status of SPVC connections (`up` or `down`). For syntax information, see the *Stinger Reference*.

With the `-a` option, the system shows all target SPVC addresses of all ATM interfaces. For example:

```
admin> spvcshow -a
Slot/Port Stat SPVC ATM address
  2 /  1  up    39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:7c:92:b7:3d:01:00
  2 /  2  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:7c:92:b7:3d:02:00
  2 /  3  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:7c:92:b7:3d:03:00
  2 /  4  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:7c:92:b7:3d:04:00
  2 /  5  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:7c:92:b7:3d:05:00
  2 /  6  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:7c:92:b7:3d:06:00
  2 /  7  up    39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:7c:92:b7:3d:07:00
  2 /  8  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:7c:92:b7:3d:08:00
  2 /  9  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:7c:92:b7:3d:09:00
  2 / 10  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:7c:92:b7:3d:0a:00
  2 / 11  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:7c:92:b7:3d:0b:00
  2 / 12  up    39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:7c:92:b7:3d:0c:00
 ...
 14 / 17  up    39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:0e:00:00:00:11:00
 14 / 18  up    39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:0e:00:00:00:12:00
 14 / 19  up    39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:0e:00:00:00:13:00
 14 / 20  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:0e:00:00:00:14:00
 14 / 21  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:0e:00:00:00:15:00
 14 / 22  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:0e:00:00:00:16:00
 14 / 23  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:0e:00:00:00:17:00
 14 / 24  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:0e:00:00:00:18:00
 17 /  1  up    39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:09:7c:9e:00:01:00
 17 /  2  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:09:7c:9e:00:02:00
 18 /  1  up    39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:09:7c:9e:00:f1:00
 18 /  2  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:09:7c:9e:00:f2:00
```

The `-s` and the `-p` options enable you to display the same information as the `-a` option, but to restrict the output to addressees on a specific slot or slot-port

combination. For example, the following command displays the addresses of a trunk module in slot 17:

```
admin> spvcshow -s 17
Slot/Port Stat SPVC ATM address
17 /  1  up    39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:09:7c:9e:00:01:00
17 /  2  down  39:84:0f:80:01:bc:72:00:01:09:7c:9e:00:ff:09:7c:9e:00:02:00
```

Monitoring failing SPVCs

The `spvcstat` command displays information about call failures and failing SPVCs. An SPVC is considered failing if it is active, but its current operational status does not indicate an established connection. For example:

```
admin> spvcstat
Call Failures = 88
Currently Failing PVCCs = 1
Currently Failing PVPCs = 1
```

Displaying signal statistics

The `atmsig` command clears ATM signaling statistics for an interface or displays signaling by interface or by slot and interface. Without any options on the command line, this command displays usage information.

The following sample command displays ATM statistics for interface 11:

```
admin> atmsig -i 11
Physical Address = { 1 17 1 }
Interface = 11
SSCOP Connections Events = 0
SSCOP Errored PDUs = 0
Received Call Setup Attempts = 0
Transmitted Call Setup Attempts = 7
Received Unavailable Routes = 0
Transmitted Unavailable Routes = 0
Received Unavailable Resources = 0
Transmitted Unavailable Resources = 0
Received Called Party Rejects = 0
Transmitted Called Party Rejects = 0
Received Msg Errors = 0
Transmitted Msg Errors = 0
Received Calling Party Rejects = 0
Transmitted Calling Party Rejects = 0
Received Timer Expired = 0
Transmitted Timer Expired = 0
Received Restarts = 0
Transmitted Restarts = 0
Incoming SVCs established = 0
Outgoing SVCs established = 6
Configured Signalling Type = pnni1dot0
Actual Signalling Type = pnni1dot0
Configured UNI Side = other
Actual UNI Side = symmetric
```

The following sample command clears the signaling statistics displayed in the preceding example.

```
admin> atmsig -c 11
```

Displaying CAC bandwidth allocation statistics

To ensure that the guaranteed characteristics can be delivered, Stinger units use a form of connection admission control (CAC), which keeps track of how much guaranteed bandwidth has been allocated and allows you to specify an oversubscription factor for trunk ports. For more information about CAC, see the *Stinger ATM Configuration Guide*.

To display CAC bandwidth allocation statistics, use the `atmcacstat` debug command. For the system to respond to this command, your `user` profile must be enabled with debug privileges. For information on enabling debug privileges see "Enabling debug permissions" on page A-1. For syntax information, see the *Stinger Reference*.

To display bandwidth allocation by slot, use the `-b` option. For example:

```
admin> atmcacstat -b
BANDWIDTH INFORMATION FOR SLOT 1
UP STREAM
    Total B/W Kbits/sec        : 70000
    Guaranteed B/W Kbits/sec   : 44000
    Allocated Guaranteed B/W   : 40000
    Available Guaranteed B/W   : 4000
DN STREAM
    Total B/W Kbits/sec        : 155520
    Guaranteed B/W Kbits/sec   : 155520
    Allocated Guaranteed B/W   : 40000
    Available Guaranteed B/W   : 115520
BANDWIDTH INFORMATION FOR SLOT 2
UP STREAM
    Total B/W Kbits/sec        : 70000
    Guaranteed B/W Kbits/sec   : 44000
    Allocated Guaranteed B/W   : 0
    Available Guaranteed B/W   : 44000
DN STREAM
    Total B/W Kbits/sec        : 155520
    Guaranteed B/W Kbits/sec   : 155520
    Allocated Guaranteed B/W   : 0
    Available Guaranteed B/W   : 155520
```

To display the CAC bandwidth allocation for the trunk module ports, use the `-p` option. For example:

```
admin> atmcacstat -p
CONTROL MODULE TRUNK PORTS B/W CONFIG
PORT {1 17 1} (oc3-atm-trunk-daughter-card) (INACTIVE) (PRIMARY)
Stream  Total BW        Gtd BW  Gtd Allocated   Gtd Available
UP      155520          155520  0               155520
DN      155520          155520  0               155520

PORT {1 17 2} (oc3-atm-trunk-daughter-card) (ACTIVE) (PRIMARY)
Stream  Total BW        Gtd BW  Gtd Allocated   Gtd Available
```

```
UP      155520          155520  0               155520
DN      155520          155520  0               155520

PORT {1 18 1} (ds3-atm-trunk-daughter-card) (ACTIVE) (PRIMARY)
Stream  Total BW        Gtd BW  Gtd Allocated   Gtd Available
UP      44223           44223   0               44223
DN      44223           44223   0               44223

PORT {1 18 2} (ds3-atm-trunk-daughter-card) (ACTIVE) (PRIMARY)
Stream  Total BW        Gtd BW  Gtd Allocated   Gtd Available
UP      44223           44223   40000           4223
DN      44223           44223   40000           4223
```

To display real-time CAC bandwidth allocation, use the `-r` option:

```
admin> atmcacstat -r
```

Connection	Stream	QOS	Peak Rate	Sustainable Rate	Count
vc-6-2-0-70	UP	CBR	15	0	2
vc-6-2-0-70	DN	CBR	15	0	2
spvc-1-1-1-1.1	UP	CBR	10	10	2
spvc-1-1-1-1.1	DN	CBR	10	10	2
spvc-1-1-1-1.2	UP	CBR	10	10	2
spvc-1-1-1-1.2	DN	CBR	10	10	2
lim-1-1-ckt-5	UP	CBR	10	10	2
lim-1-1-ckt-5	DN	CBR	10	10	2
spvc-1-1-1-1.3	UP	CBR	10	10	2
spvc-1-1-1-1.3	DN	CBR	10	10	2
lim-1-1-ckt-6	UP	CBR	10	10	2
lim-1-1-ckt-6	DN	CBR	10	10	2
spvc-1-1-1-1.4	UP	CBR	10	10	2
spvc-1-1-1-1.4	DN	CBR	10	10	2
lim-1-1-ckt-7	UP	CBR	10	10	2
lim-1-1-ckt-7	DN	CBR	10	10	2
lim-1-1-ckt-8	UP	CBR	10	10	2
lim-1-1-ckt-8	DN	CBR	10	10	2

To display bandwidth allocation for a specific service category, use the `-c` option with one of the following values for service category: 0 for constant bit rate (CBR), 1 for real-time variable bit rate (RT-VBR), 2 for Nonreal-time variable bit rate (NRT-VBR), or 3 for unspecified bit rate (UBR).

```
admin> atmcacstat -c 0
```

```
Quality of Service : CBR
```

Connection	Stream	Peak Rate	Sustainable Rate	Count
vc-6-2-0-70	UP	15	0	2
vc-6-2-0-70	DN	15	0	2
spvc-1-1-1-1.1	UP	10	10	2

```
spvc-1-1-1-1.1    DN        10              10                    2
spvc-1-1-1-1.2    UP        10              10                    2
spvc-1-1-1-1.2    DN        10              10                    2
lim-1-1-ckt-5     UP        10              10                    2
lim-1-1-ckt-5     DN        10              10                    2
spvc-1-1-1-1.3    UP        10              10                    2
spvc-1-1-1-1.3    DN        10              10                    2
lim-1-1-ckt-6     UP        10              10                    2
lim-1-1-ckt-6     DN        10              10                    2
spvc-1-1-1-1.4    UP        10              10                    2
spvc-1-1-1-1.4    DN        10              10                    2
lim-1-1-ckt-7     UP        10              10                    2
lim-1-1-ckt-7     DN        10              10                    2
lim-1-1-ckt-8     UP        10              10                    2
lim-1-1-ckt-8     DN        10              10                    2
```

To display all bandwidth characteristics for all active connections, use the **-a** option. For example:

```
admin> atmcacstat -a

Connection       Stream   QOS       Peak Rate   Sustainable Rate   Count
rcc-17-1-0-18    UP       NRT-VBR   384         192                1
                 DN       NRT-VBR   384         192                1
rcc-18-2-0-18    UP       NRT-VBR   384         192                1
                 DN       NRT-VBR   384         192                1
sig-17-1-0-5     UP       NRT-VBR   16          16                 1
                 DN       NRT-VBR   16          16                 1
sig-17-2-0-5     UP       NRT-VBR   16          16                 1
                 DN       NRT-VBR   16          16                 1
sig-18-1-0-5     UP       NRT-VBR   16          16                 1
                 DN       NRT-VBR   16          16                 1
sig-18-2-0-5     UP       NRT-VBR   16          16                 1
                 DN       NRT-VBR   16          16                 1
rcc-17-2-0-18    UP       NRT-VBR   384         192                1
                 DN       NRT-VBR   384         192                1
rcc-18-1-0-18    UP       NRT-VBR   384         192                1
                 DN       NRT-VBR   384         192                1
```

Displaying ATM connection failures

To display information about ATM connection failures, use the `atmconnectionfailures` command. For example:

```
admin> atmConnectionFailures
Profile Reason
4-2-17-1 NG/VPI/VCI 152/0/35 or 801/202/36 is not valid for VCC
4-3-17-1 NG/VPI 153/0 or 801/203 is not valid for VCC
```

Displaying QoS statistics

To display the quality of service (QoS) statistics on ATM connections, use the `atmqos` command. For syntax information, see the *Stinger Reference*.

To display all ATM connections in a Stinger unit with QoS settings, use the `-a` option. For example:

```
admin> atmqos -a
```

Td Index	QoS Name	Category	PCR (Cells Per Second)	SCR (Cells Per Second)
1	default	UBR	0	-
2	default-ctl	NRT_VBR	37	37
3	default-rcc	NRT_VBR	905	452
392	ATMQOS392	UBR	96000	-
416	ATMQOS416	RT_VBR	1000	1000

For details about the output of this command, see the *Stinger Reference*.

To display all connections that use a specified QoS name, use the `-c` option. For example:

```
admin> atmqos -c atmqos416
vc-11-1-0-35
Total Number Of Connections : 1
```

To display QoS statistics for a specific QoS name, use the `-d` option. For example:

```
admin> atmqos -d atmqos416
Traffic Descriptor    : 416
Traffic Type          : NO_CLP_SCR
PCR(Cells Per Second) : 1000
SCR                   : 1000
MBS                   : 5
QOS Class             : 0
ATM Service Category  : RT_VBR
```

Monitoring PNNI nodes

You can use profiles and commands to monitor PNNI node configuration, operations, and statistics. For information about configuring PNNI operations on a Stinger unit, see the *Stinger Private Network-to-Network Interface (PNNI) Supplement*.

Table 7-2 lists the profiles and commands that you use to monitor PNNI operations.

Table 7-2. Commands and profiles for monitoring PNNI operations

Command or profile	Used for
`atm-if-stat` profile	"Verifying the PNNI link" on page 7-19
`pnnidisplay` command	"Displaying general PNNI information" on page 7-20
`pnniinterfacedisplay` command	"Displaying PNNI interface information" on page 7-21
`pnnilinkdisplay` command	"Displaying information about PNNI logical links" on page 7-22
`pnnimapdisplay` command	"Displaying information about the PNNI hierarchy" on page 7-24
`pnninbrdisplay` command	"Displaying details about neighbor nodes" on page 7-27
`pnninodedisplay` command	"Displaying local node information" on page 7-28
`pnninodetopology` command	"Displaying the PNNI topology database" on page 7-32
`pnniptsestatus` command	"Displaying the PNNI routing table" on page 7-33
`pnnirouteBase` command `pnnireachableaddr` command	"Displaying PNNI interface information" on page 7-21
`pnnirouteBase` command	"Displaying PNNI interface information" on page 7-21

Verifying the PNNI link

To verify that PNNI signaling and the PNNI link are active, open the `atm-if-stat` profile for the interface. For example:

```
admin> read atm-if-stat { { 1 18 1 } 0 }
ATM-IF-STAT/{ { shelf-1 trunk-module-2 1 } 0 } read

admin> list
[in ATM-IF-STAT/{ { shelf-1 trunk-module-2 1 } 0 }]
address* = { { shelf-1 trunk-module-2 1 } 0 }
if-number = 11
nailed-group = 851
port-state = up
signalling-state = up
pnni-link-state = up
```

The preceding profile indicates that the signaling and PNNI link state are established. For a port that has not been configured for PNNI, those settings indicate that signaling and PNNI links have not been configured. For example:

```
admin> read atm-if-stat { { 1 18 2 } 0 }
ATM-IF-STAT/{ { shelf-1 trunk-module-2 2 } 0 } read
admin> list
[in ATM-IF-STAT/{ { shelf-1 trunk-module-2 2 } 0 }]
address* = { { shelf-1 trunk-module-2 2 } 0 }
if-number = 12
nailed-group = 852
port-state = up
signalling-state = not-configured
pnni-link-state = not-configured
```

For details on the parameters, see the *Stinger ATM Configuration Guide*.

Displaying general PNNI information

The pnnidisplay command displays general information about PNNI implementation, including internal counters. The command does not have any command options. The following sample output shows that PNNI 1.0 is supported, and that the system failed to compute routes 148 times because the destination was unreachable:

```
admin> pnnidisplay
HighestVersion           = Version1point0
LowestVersion            = Version1point0
DtlCountOriginator       = 0
DtlCountBorder           = 0
CrankbackCountOriginator = 0
CrankbackCountBorder     = 0
AltRteCountOriginator    = 0
AltRteCountBorder        = 0
RteFailCountOriginator   = 148
RteFailCountBorder       = 0
RteFailUnreachOrg        = 148
RteFailUnreachBrdr       = 0
```

Field	Indicates
HighestVersion	Highest version of the PNNI protocols supported in the unit.
LowestVersion	Lowest version of the PNNI protocols supported in the unit.
DtlCountOriginatr	Number of destination transit list (DTL) stacks the unit has originated and placed in PNNI signaling messages.
DtlCountBorder	Number of partial DTL stacks the unit has added into signaling messages as an entry border node.
CrankbackCount Originator	Number of connection setup messages, including DTL stacks the unit has originated, that have cranked back to this node.
CrankbackCountBorder	Number of connection setup messages, including DTL stacks the unit has added as an entry border node, that have cranked back to this node.

Field	Indicates
AltRteCountOriginator	Number of alternate DTL stacks the unit has computed and placed into signaling messages it originated.
AltRteCountBorder	Number of alternate partial DTL stacks the unit has computed and placed into signaling messages as an entry border node.
RteFailCountOriginator	Number of times the unit failed to compute a viable DTL stack as originator for a call. This value indicates the number of times a call was cleared due to originator routing failure.
RteFailCountBorder	Number of times the unit failed to compute a viable partial DTL stack as an entry border node for a call. This value indicates the number of times a call was either cleared or cranked back from this node due to border routing failure.
RteFailUnreachOrg	Number of times the unit failed to compute a viable DTL stack as originator because the destination was unreachable. This value indicates those calls that were cleared with cause 2 (specified transit network unreachable) or cause 3 (destination unreachable) in the cause information element.
RteFailUnreachBrdr	Number of times the unit failed to compute a viable partial DTL stack as entry border node because the target of the path calculation was unreachable. This value indicates those calls that were cleared or cranked back with cause 2 (specified transit network unreachable) or cause 3 (destination unreachable) in the cause information element.

Displaying PNNI interface information

To display the configuration of PNNI physical interfaces, use the `pnniinterfacedisplay` command. The command does not have any command options. The following sample output shows that both ports of the trunk module in slot 17 are configured for PNNI:

```
admin> pnniinterfacedisplay
Port  PhyAddr       IntIndex      Node          AggrToken     VpCap
801   {1 17 1}      11            1             0             Y

   Cbr Wt        RtVbr Wt      NrtVbr Wt     Abr Wt        Ubr Wt
   5040          5040          5040          5040          5040

   Port  PhyAddr       IntIndex      Node          AggrToken     VpCap
   802   {1 17 2}      12            1             0             Y

   Cbr Wt        RtVbr Wt      NrtVbr Wt     Abr Wt        Ubr Wt
```

```
   5040          5040          5040          5040          5040
```

Field	Indicates
Port	Nailed group number associated with the physical port.
PhyAddr	Physical address of the trunk port in the following format: { *shelf-n slot-n item-n* }
IntIndex	Entry number in the interface table.
Node	PNNI node index. Only node index 1 is currently supported.
AggrToken	Configured aggregation token for this interface.
VpCap	Y if the interface is capable of having virtual path connections (VPCs) established within it, or N if it is not.
Cbr Wt	Configured administrative weight of this interface for the constant bit rate (CBR) service category.
RtVbr Wt	Configured administrative weight of this interface for the real-time variable bit rate (RT-VBR) service category.
NrtVbr Wt	Configured administrative weight of this interface for the nonreal-time variable bit rate (NRT-VBR) service category.
Abr Wt	Configured administrative weight of this interface for the available bit rate (ABR) service category.
Ubr Wt	Configured administrative weight of this interface for the unspecified bit rate (UBR) service category.

Displaying information about PNNI logical links

A PNNI *logical link* is a logical representation of the connectivity between two logical nodes, including the physical link and virtual path connection. The `pnnilinkdisplay` command displays information about the operation of logical links attached to the local PNNI node and the relationship to nodes on the other end of the links. For syntax information, see the *Stinger Reference*.

With no options on the command line, the command prints a summary of all PNNI logical links. For example, the following output shows two logical links, one on each of the configured trunk ports in slot 17. The first link is attempting Hello protocol exchanges with its neighbors, and the second is established as a lowest-level horizontal link.

```
admin> pnnilinkdisplay
Node PortId     PhysicalAddr  IntfIndex    LinkType     HelloState
   1    801       {1 17 1}       11           Unknown      Attempt
   RemoteNodeId
   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

Node PortId    PhysicalAddr   IntfIndex  LinkType      HelloState
1    802       {1 17 2}       12         Lowest horiz  Twoway inside
   RemoteNodeId
   60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:38:ff:b6:ca:99:00:00:00
```

With the `-d` option, the command displays additional details. For example, the following output shows that the link on the first port in slot 17 (port ID 801) has

transmitted 121 Hello packets, but has received no information from the remote node.

```
admin> pnnilinkdisplay -d 1 801
Node PortId     PhysicalAddr   IntfIndex      LinkType       HelloState
1    801        {1 17 1}       11             Unknown        Attempt
   RemoteNodeId
   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
   RemotePortId   DerAggrToken   SvccRccIndex   RcvHellos      XmtHellos
     0              0              0              0              121
   UpnodeId
   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

   UpnodeAtmAddress
   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

   CommonPeerGroupId                              LinkVersion
   00:00:00:00:00:00:00:00:00:00:00:00:00:00       1
```

Field	Indicates
Node	PNNI node index. Only node index 1 is currently supported.
PortId	Dedicated (nailed) group number associated with the physical port. The node index (1) and port ID identify the interface to which the link is attached.
PhysicalAddr	Physical address of the trunk port in the following format: { *shelf-n slot-n item-n* }
IntIndex	Entry number in the interface table for the interface to which the logical link corresponds. The value is valid only for LinkType values of Unknown, Lowest Level Horizontal Link, and Lowest Level Outside Link. All other link types display a zero value.
LinkType	Type of logical link. Possible types are Unknown, Lowest Level Horizontal Link, Horizontal link to/from LGN, Lowest Level Outside Link, Uplink, and Outside link and Uplink. (An *uplink* is a link to a higher-level node.)
HelloState	State of the Hello protocol exchange across the link or the state of the corresponding logical group node (LGN) horizontal link Hello exchange. For uplinks, the field displays NA. Other link types have the following valid values: NA, Down, Attempt, Oneway Inside, Twoway Inside, Oneway Outside, Twoway Outside, and Common Outside.
RemoteNodeId	Node ID of the neighboring node on the other end of the link. The value is valid only for LinkType values of Lowest Level Outside Link or Uplink. If the node at the other end of an uplink (*upnode*) has not yet been identified, or if the LinkType is Lowest Level Horizontal Link, the field displays zero.

Field	Indicates
RemotePortId	Port ID of the port at the other end of the link. If the LinkType is Outside link and Uplink, the field shows the port ID assigned by the lowest-level neighbor node to identify the outside link. If the remote port ID is unknown or if the LinkType is Uplink, the field displays zero.
DerAggrToken	Derived aggregation token value on the link. For horizontal links between lowest-level nodes, the value is always zero.
SvccRccIndex	Switched virtual channel connection (SVCC)-based routing control channel (RCC) used to exchange information with the neighboring peer logical group node. (*Not currently supported*.)
RcvHellos	Number of Hello packets received over this link. The value is valid for horizontal and outside links between lowest-level nodes and for links of unknown type. Other link types display zero.
XmtHellos	Number of Hello packets transmitted over this link. The value is valid for horizontal and outside links between lowest-level nodes and for links of unknown type. Other link types display zero.
UpnodeId	Node ID of the neighbor node. For horizontal links, or when the link type or upnode is not yet known, the field displays zero.
UpnodeAtmAddress	ATM end-system address used to establish connections to the upnode. For horizontal links, or when the link type or upnode is not yet known, the field displays zero.
CommonPeerGroupId	Peer group ID of the lowest-level common peer group in the hierarchy of the neighboring node and the local node. For horizontal links, or when the link type or common peer group is not yet known, the field displays zero.
LinkVersion	Version of PNNI routing protocol used to exchange information over this link. If communication with the neighbor node has not yet been established, or if the link type is Uplink or Link to/from LGN, the field displays Unknown.

Displaying information about the PNNI hierarchy

The `pnnimapdisplay` command displays information about the PNNI hierarchy. You can use this information to find and analyze the operation of all links and nodes within the PNNI hierarchy from the perspective of a local node. For syntax information, see the *Stinger Reference*.

With no options on the command line, the command displays information about links between local and remote nodes. In the following sample output, the system is reporting a link on each of its active PNNI ports, with details about the originating and remote IDs:

```
admin> pnnimapdisplay
```

```
Nd Index
1  1

OriginatingNodeId                                                OrigPortId
60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:30:ff:18:dd:98:00:00:00       802

RemoteNodeId                                                      RmtPortId
60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:38:ff:b6:ca:99:00:00:00       801

Nd Index
1  1

OriginatingNodeId                                                OrigPortId
60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:38:ff:b6:ca:99:00:00:00       801

RemoteNodeId                                                      RmtPortId
60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:30:ff:18:dd:98:00:00:00     802
```

With the **-d** option, the command displays additional details about each link. In the following example, the command displays information about the link originating on its port 802, including the type of link and the routing metrics and attributes from this node to the specified remote node:

```
admin> pnnimapdisplay -d 1
Nd Index
1  1

OriginatingNodeId                                                OrigPortId
60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:30:ff:18:dd:98:00:00:00      802

RemoteNodeId                                                      RmtPortId
60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:38:ff:b6:ca:99:00:00:00       801

MapType          PeerGroupId
HorizontalLink   60:39:84:0f:80:01:bc:72:00:01:31:a3:99:00

AggrToken        VpCap            PtseId           MTag
0                1                4                1118482

Qos     Dir     AdmWt      MCR       ACR       CTD       CDV      CLR0   CLR0+1
Cbr     Out      5040   366792    366792      6890   Unused         8        8
Rtvbr   Out      5040   366792    366792      6890   Unused         8        8
NrtVbr  Out      5040   366792    366792      6890   Unused         8        8
Abr     Out      5040   366792    366792      6890   Unused         8        8
Ubr     Out      5040   366792    366792      6890   Unused         8        8
Cbr     Out      5040   366792    366792      1574     1554         8        8
Rtvbr   Out      5040   366792    366792      1574     1554         8        8
NrtVbr  Out      5040   366792    366792      1574     1554         8        8
Abr     Out      5040   366792    366792      1574     1554         8        8
Ubr     Out      5040   366792    366792      1574     1554         8        8
Cbr     Out      5040   366792    366792       674      654         8        8
Rtvbr   Out      5040   366792    366792       674      654         8        8
NrtVbr  Out      5040   366792    366792       674      654         8        8
```

```
Abr     Out      5040    366792    366792       674       654         8         8
Ubr     Out      5040    366792    366792       674       654         8         8
```

Field	Indicates
Nd	PNNI node index. Only node index 1 is currently supported.
Index	Map index, required because a specific node and port pair can have multiple entries for nodal connectivity, in addition to any entry for a horizontal link or uplink.
OriginatingNodeId	PNNI node ID of the originating node represented in this entry.
OrigPortId	Port ID as assigned by the originating node.
RemoteNodeId	PNNI node ID of the remote node at the other end of the link from the originating node. If unknown, the field displays zero.
RmtPortId	Port ID as assigned by the remote node at the other end of the link from the originating node. If the ID is unknown, the field displays zero.
MapType	Type of PNNI entity being described by this entry in the map table. Valid types are HorizontalLink, Uplink, and Node.
PeerGroupId	Peer group ID of the originating node.
AggrToken	Derived aggregation token value for this link. For nodes and for horizontal links between lowest-level nodes, the field displays zero.
VPCap	A value of 1 indicates that virtual path connections (VPCs) can be established across the PNNI entity. A value of zero indicates that VPCs cannot be established.
PtseId	PNNI state topology element (PTSE) ID for the PTSE that contains the information group(s) describing the PNNI entity. The PTSE is originated by the originating node.
MTag	Integer that represents a set of traffic parameters. The zero value indicates that no metrics are associated with the link or nodal connectivity.
Qos	Service categories to which this set of metrics applies.
Dir	Direction in which metrics apply (`In` or `Out`).
AdmWt	Administrative weight of the service category.
MCR	Maximum cell rate in cells per second for the service category.
ACR	Available cell rate in cells per second for the service category.
CTD	Maximum cell transfer delay in microseconds for the service category.
CDV	Cumulative cell delay variation in microseconds for the service category.

Field	Indicates
CLR0	Cell loss ratio for traffic with a cell loss priority (CLP) level of 0 (zero) for the service category.
CLR0+1	Cumulative cell loss ratio for traffic with CLP level of 0 + 1 for the service category.

Displaying details about neighbor nodes

A PNNI *neighbor node* is a node that is directly connected to a particular node via a logical link. The `pnninbrdisplay` command displays information about the relationship between the local node and a neighboring node within the same peer group. For syntax information, see the *Stinger Reference*.

With no options on the command line, the command displays the PNNI node ID and state of its neighbor peers. In the following sample output, the system recognizes one neighbor node and identifies the link to that neighbor as fully established:

```
admin> pnninbrdisplay
Node PeerState      PeerPortCount
1    Full           1

     PeerNodeId
     60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:38:ff:b6:ca:99:00:00:00
```

With the `-d` option, the `pnninbrdisplay` command displays additional details about the neighbor node, including statistics about packet exchanges with the neighbor, as shown in the following sample output:

```
admin> pnninbrdisplay -d
Node PeerState      PeerPortCount
1    Full           1

PeerNodeId
60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:38:ff:b6:ca:99:00:00:00

PeerSvcRccIdx  PeerRcvDbSums  PeerXmtDbSums  PeerRcvPtsps PeerXmtPtsps
0              2              3              64           64

PeerRcvPtseReq PeerXmtPtseReq PeerRcvPtseAck PeerXmtPtseAck
0              1              48             7
```

Field	Indicates
Node	PNNI node index. Only node index 1 is currently supported.
PeerState	State of the local node's neighboring peer state machine associated with PeerNodeId field. The field can display NP Down (neighboring peer is down), Negotiating, Exchanging, Loading, or Full.
PeerPortCount	Total number of ports to the neighboring peer. If the peer communicates only through an SVCC-based RCC, the field displays zero. (*SVCC-based RCCs are currently not supported.*)
PeerNodeId	PNNI node ID of the neighboring peer node.

Field	Indicates
PeerSvccRccIndex	Identifies the SVCC-based RCC being used to communicate with the neighboring peer. (*SVCC-based RCCs are currently not supported.*) If both the local node and the neighboring peer are lowest-level nodes, the field displays zero.
PeerRcvDbSums	Number of database summary packets received from the neighboring peer.
PeerXmtDbSums	Number of database summary packets transmitted to the neighboring peer.
PeerRcvPtsps	Number of PNNI topology state packets (PTSPs) received from the neighboring peer.
PeerXmtPtsps	Number of PTSPs retransmitted to the neighboring peer.
PeerRcvPtseReq	Number of PTSE Request packets received from the neighboring peer.
PeerXmtPtseReq	Number of PTSE Request packets transmitted to the neighboring peer.
PeerRcvPtseAck	Number of PTSE Ack (acknowledgement) packets received from the neighboring peer.
PeerXmtPtseAck	Number of PTSE Ack packets transmitted to the neighboring peer.

Displaying local node information

With the current software version, Stinger units support a single logical node, which is always a lowest-level node. The `pnninodedisplay` command displays information about factors that affect the operation of the PNNI logical node. For syntax information, see the *Stinger Reference*.

With no options on the command line, the command identifies the node and displays some state information. Following is some sample output:

```
admin> pnninodedisplay
Node NodeId
1    60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:30:ff:18:dd:98:00:00:00

OperStat        DBOverload      Ptses
    UP              NO              21
```

With the `-d` option, the command displays many additional fields about the configuration and current state of the logical node. For example:

```
admin> pnninodedisplay -d
Node NodeId
1    60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:30:ff:18:dd:98:00:00:00

     OperStat        DBOverload      Ptses
     UP              NO              21

     NodeLevel       LowestLevel     AdminStatus     DomainName
     96              YES             UP              stinger1r
```

```
AtmAddress
39:84:0f:80:01:bc:72:00:01:31:a3:99:30:ff:18:dd:98:00:00:00

PeerGroupId                                    RestrictedTransit
60:39:84:0f:80:01:bc:72:00:01:31:a3:99:00      NO

PglLeaderPri    PglState        PglTimeStamp
0               Oper not PGL    01/01/1990 00:00:00

PreferredPgl
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

PeerGroupLeader
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
```

Field	Indicates
`Node`	PNNI node index. Only node index 1 is currently supported.
`NodeId`	PNNI node ID of the local node.
`OperStat`	Indication of the operational status of the node (Up or Down).
`DBOverload`	Whether the node is currently operating in topology database overload state (Yes or No).
`Ptses`	Total number of PNNI topology state elements (PTSEs) in the node's topology database at this time.
`NodeLevel`	Number from 0 to 104 indicating the level of PNNI hierarchy at which the node exists.
`LowestLevel`	Whether the node acts as a lowest-level node (Yes or No).
`AdminStatus`	Administrative status of the node. Up indicates that the node is allowed to become active. Down means the node is inactive and is not allowed to become active.
`DomainName`	Name of the node's PNNI routing domain. All lowest-level nodes with the same domain name are presumed to be connected.
`AtmAddress`	Node's ATM address.
`PeerGroupId`	Node's peer group ID.
`RestrictedTransit`	Whether the node is restricted to not allowing support of SVCs transiting this node (Yes or No).
`PglLeaderPri`	Number indicating the leadership priority value that the node advertises. With the current software version, zero is displayed, because the node cannot become a peer group leader.
`PglState`	State of the node regarding peer group leader election with the peer group. Following are valid values: `Starting`, `Awaiting`, `Awaiting Full`, `Initial Delay`, `Calculating`, `Await Unanimity`, `Oper PGL`, `Oper Not PGL`, `Hung Election`, `Await Reelection`.

Field	Indicates
PglTimeStamp	Time at which the current peer group leader was established.
PreferredPgl	Node that the local node prefers as leader of its peer group.
PeerGroupLeader	Current peer group leader.

Displaying information about other nodes

The pnninodetopology command displays the information about nodes that the local node has obtained from nodal information PTSEs. For syntax information, see the *Stinger Reference*.

With no options on the command line, the command displays the node index and PNNI node ID (map node ID), as shown in the following output:

```
admin> pnninodetopology
Node MapNodeId
1    60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:30:ff:18:dd:98:00:00:00
1    60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:38:ff:b6:ca:99:00:00:00
```

With the -d option, the command displays additional details about the nodes, as shown in the following sample output:

```
admin> pnninodetopology -d
Node MapNodeId
1    60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:30:ff:18:dd:98:00:00:00

     PeerGroupId
     60:39:84:0f:80:01:bc:72:00:01:31:a3:99:00

     NodeAtmAddress
     39:84:0f:80:01:bc:72:00:01:31:a3:99:30:ff:18:dd:98:00:00:00

     RestrictedTransit       NodeComplexRep          RestrictedBranching
     NO                      NO                      NO

     NodeDatabaseOverload    IAMLeader               LeadershipPriority
     NO                      NO                      0

     PreferredPgl
     00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

     ParentNodeId
     00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

     ParentAtmAddress
     00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

     NodeParentPeerGroupId
     00:00:00:00:00:00:00:00:00:00:00:00:00:00

     ParentPglNodeId
     00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
```

```
Node MapNodeId
1    60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:38:ff:b6:ca:99:00:00:00

     PeerGroupId
     60:39:84:0f:80:01:bc:72:00:01:31:a3:99:00

     NodeAtmAddress
     39:84:0f:80:01:bc:72:00:01:31:a3:99:38:ff:b6:ca:99:00:00:00

     RestrictedTransit       NodeComplexRep          RestrictedBranching
     NO                      NO                      NO

     NodeDatabaseOverload    IAMLeader               LeadershipPriority
     NO                      NO                      0

     PreferredPgl
     00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

     ParentNodeId
     00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

     ParentAtmAddress
     00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

     NodeParentPeerGroupId
     00:00:00:00:00:00:00:00:00:00:00:00:00:00

     ParentPglNodeId
     00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
```

Field	Indicates
Node	PNNI node index. Only node index 1 is currently supported.
MapNodeId	PNNI node ID of the node being represented.
PeerGroupId	PNNI peer group ID of the node being represented.
NodeAtmAddress	ATM address of the node being represented.
RestrictedTransit	Whether the node is restricted to not allowing support of SVCs transiting this node (Yes or No).
NodeComplexRep	Whether the node uses complex node representation (Yes or No).
RestrictedBranching	Whether the node is restricted from supporting additional point-to-multipoint branches (Yes or No).
NodeDatabaseOverload	Whether the node is currently operating in topology database overload state (Yes or No).
IAmLeader	Whether the originating node claims to be leader of its peer group (Yes or No).

Field	Indicates
LeadershipPriority	Number indicating the leadership priority value the node advertises.
PreferredPgl	Node that the local node prefers as leader of its peer group.
ParentNodeId	If the node is peer group leader, this field displays the node ID of the parent logical group node (LGN). If the node is not peer group leader, it displays zero.
ParentAtmAddress	If the node is peer group leader, this field displays the ATM address of the parent LGN. If the node is not peer group leader, it displays zero.
NodeParentPeerGroupId	If the node is peer group leader, this field displays the node's parent peer group ID. If the node is not peer group leader, it displays zero.
ParentPglNodeId	If the node is peer group leader, this field displays the node ID of the peer group leader of the parent peer group. If the node is not peer group leader, it displays zero.

Displaying the PNNI topology database

The pnniptsestatus command displays PNNI topology state elements (PTSEs) in the local node's topology database. For syntax information, see the *Stinger Reference*.

With no options on the command line, the command displays the current topology database, as shown in the following sample output:

```
admin> pnniptsestatus
OrigNodeId
60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:30:ff:18:dd:98:00:00:00

Node PtseId (hex)   SeqNum    LifeTime  CheckSum       PtseType
1    1              47        3600      11143          NodalInfo
1    2              60        3600      51918          InternalAddr
1    4              2         3600      46441          HorizontalLink
1    5              4         3600      7165           InternalAddr
1    6              3         3600      52636          InternalAddr
1    7              2         3600      15160          InternalAddr
1    8              3         3600      61997          InternalAddr
1    9              8         3600      62930          InternalAddr
1    a              5         3600      25143          InternalAddr
1    b              4         3600      12231          InternalAddr
1    c              10        3600      37892          InternalAddr
1    d              10        3600      37791          InternalAddr
1    e              9         3600      37691          InternalAddr
1    11             1         3600      6042           InternalAddr


OrigNodeId
60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:38:ff:b6:ca:99:00:00:00
```

```
Node PtseId (hex)   SeqNum    LifeTime  CheckSum       PtseType
1    1              43        3308      56751          NodalInfo
1    2              50        1658      43086          InternalAddr
1    4              41        2678      33703          InternalAddr
1    5              43        2145      33718          InternalAddr
1    6              43        2061      33721          InternalAddr
1    7              42        1850      33667          InternalAddr
1    a              2         3301      46435          HorizontalLink
```

You can specify an originating node ID on the command line, use an option to retrieve information only about a specific PTSE type, or to retrieve specific PTSE types originated by a specific node. For example, the following sample command displays information only about horizontal link PTSEs:

```
admin> pnniptsestatus -h
OrigNodeId
60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:30:ff:18:dd:98:00:00:00

Node PtseId (hex)   SeqNum    LifeTime  CheckSum       PtseType
1    4              2         3600      46441          HorizontalLink


OrigNodeId
60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:38:ff:b6:ca:99:00:00:00

Node PtseId (hex)   SeqNum    LifeTime  CheckSum       PtseType
1    a              2         3301      46435          HorizontalLink
```

Field	Indicates
OrigNodeId	PNNI node ID of the node that originated the PTSE.
Node	Local node number.
PtseId	Hexadecimal value of the PTSE identifier assigned to the PTSE by the originating node.
SeqNum	Sequence of the entry in the local topology database.
LifeTime	Remaining lifetime in seconds, for the given PTSE as stated in the topology database.
Checksum	Entry's PTSE checksum as stated in the topology database.
PtseType	Type of information contained in the PTSE entry. Valid values are Other, NodalState, NodalInfo, InternalAddr, ExteriorAddr, HorizontalLinks, and Uplinks.

Displaying the PNNI routing table

The pnniroutebase command displays the number of current PNNI routes from nodes in the PNNI routing domain to valid addresses and transit networks. For example:

```
admin> pnniroutebase
pnniRouteAddrNumber     = 161
```

The pnnireachableaddr command displays a list of all reachable addresses from each node visible to the local node. For syntax information, see the *Stinger Reference*.

With no options on the command line, the command prints the entire list of reachable addresses. Following is an excerpt showing a few entries from sample output:

```
admin> pnnireachableaddr
AdvertisedNodeId
60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:30:ff:18:dd:98:00:00:00

     PortId              Index               PrefixLength (bits)
     36610               2                   152

     ReachableAddr
     39:84:0f:80:01:bc:72:00:01:18:dd:98:00:ff:18:dd:98:00:02

AdvertisedNodeId
60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:30:ff:18:dd:98:00:00:00

     PortId              Index               PrefixLength (bits)
     36610               3                   152

     ReachableAddr
     39:84:0f:80:01:bc:72:00:01:18:dd:98:00:ff:18:dd:98:00:f1

AdvertisedNodeId
60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:30:ff:18:dd:98:00:00:00

     PortId              Index               PrefixLength (bits)
     36610               4                   152

     ReachableAddr
     39:84:0f:80:01:bc:72:00:01:18:dd:98:00:ff:18:dd:98:00:f2

AdvertisedNodeId
60:a0:39:84:0f:80:01:bc:72:00:01:31:a3:99:30:ff:18:dd:98:00:00:00

     PortId              Index               PrefixLength (bits)
     36610               5                   152

     ReachableAddr
     39:84:0f:80:01:bc:72:00:01:18:dd:98:00:ff:f7:48:cf:3b:01
```

You can use a command option to display reachable addresses from a specified node or ATM address. For example, the following output shows addresses that are reachable from the specified ATM prefix:

```
admin> pnnireachableaddr -a 39:84:0f:80:01:bc:72:00:01:17:fd:27:09
AdvertisedNodeId
60:a0:39:84:0f:80:01:bc:72:00:01:17:fd:27:09:ff:e8:71:75:03:00:00

     PortId              Index               PrefixLength (bits)
     0                   1                   104
```

```
ReachableAddr
39:84:0f:80:01:bc:72:00:01:17:fd:27:09
```

Field	Indicates
AdvertisingNodeId	PNNI node ID of a node that advertises reachability to the ATM prefix displayed in the ReachableAddr field.
PortId	Port ID used from the advertising node to reach the ATM prefix displayed in the ReachableAddr field.
Index	Arbitrary index used to enumerate the addresses advertised by the advertising node.
PrefixLength	Number of significant bits in the prefix displayed in the ReachableAddr field.
ReachableAddr	ATM prefix of the reachable address.

Diagnostic Testing

8

OAM testing

Stinger units support operations, administration, and maintenance (OAM) F4 and F5 testing. ITU-T I.610 defines OAM functions.

OAM cells have following functions:

- Fault management using Alarm Indication signal (AIS), remote detection indication (RDI), loss of continuity, far-end receive failure, continuity check, and loopback OAM cells
- Performance management using forward monitoring and backward reporting OAM cells
- Activation/deactivation of performance monitoring and/or continuity check using activation/deactivation OAM cells
- System management OAM cells use by end-systems

Overview of F4 and F5 OAM tests

OAM F4 testing is a diagnostic tool for testing end-to-end and segment continuity in a virtual path connection (VPC). OAM F4 cells operate at the virtual path level. They use the following reserved virtual channel indentifiers (VCIs):

- VCI 3 for segment OAM F4 cells
- VCI 4 for end-to-end OAM F4 cells

To respond to F4 OAM segment loopback cells, the control module requires special cross-connect circuits so that it can extract the F4 OAM cells and then forward them back to the segmentation and reassembly (SAR) sublayer on the incoming slot. At the trunk module or LIM, the SAR sublayer examines the F4 OAM cells and replies with the appropriate message to the control module. Upon receiving the F4 response, the

control module forwards the F4 response to the incoming port on the trunk module or line interface module (LIM).

Note The Stinger unit does not support F4 OAM end-point tests for virtual path connections (VPCs) because the connection does not terminate on the Stinger unit.

OAM F5 cells operate at the virtual circuit level and use the payload type indicator (PTI) field to distinguish between data and OAM cells. On Stinger units, F5 OAM test flows cover either an end-to-end virtual connection or only a segment of the virtual connection.

Using the `oam` command and `atm-oam` profile to run OAM tests

You can run an F4 or F5 OAM loopback or continuity check test using the `oam` command or the `atm-oam` profile. A network peer can also activate and deactivate a continuity check test. If the system is reset or a switchover occurs, all incomplete tests are restarted.

You can run OAM tests in the following configurations:

- An F4 *or* F5 OAM loopback *or* continuity test on a particular ATM circuit
- An F4 *or* F5 OAM loopback test on all ATM circuits on a particular port on a slot
- An F4 *or* F5 OAM loopback test on all ATM circuits on a slot
- An F5 OAM loopback test on all ATM circuits with a particular virtual path identifier (VPI) and port

You can run the following tests for a virtual path connection (VPC) or virtual channel connection (VCC):

Configuration	F4	F5	Segment	End-to-end
VPC connecting point	Yes	No	Yes	No
VCC end point	Yes	Yes	Yes	Yes
VCC connecting point	Yes	Yes	Yes	No

Any cross connection can be enabled as a segment end point. However, only Stinger terminating connections can be end points on the slot and port on which they terminate. Consider the following situations:

- A virtual switching virtual path (VC-switching VPI) on a trunk port terminates on that trunk port. It therefore terminates on that control module. This type of virtual path can have both F4 segment and F4 end-to-end OAM flows.
- A virtual channel connection that terminates on a line interface module (LIM) or on a control module (through a trunk) has F5 segment and F5 end-to-end flows on the LIM or control module, respectively.
- A VPC or VCC that is switched towards a LIM port does not terminate within the Stinger system. Therefore the LIM can only be the end point for F4 and F5 segment OAM flows. The LIM will always ignore and pass through F4 and F5 end-to-end OAM flows.

Overview of the `oam` command

You can use the `oam` command to run F4 and F5 OAM loopback and continuity check tests and to display OAM entries. You use the command as follows:

- To run loopback tests, use the following command syntax:

  `oam -L slot port vpi|-l slot port vpi [vci] e|s cell-count`

- To run continuity tests, use the following command syntax:

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

- To display OAM entries in a Stinger system, use the `oam -e` command. Its syntax is as follows:

  `oam -e [slot] [port] [vpi] [vci]|-p`

- To display a subset of the entries reported by the OAM queries, use the oam -q command. Its syntax is as follows:

  `oam -q fault normal | fault ais | fault rdi | fault loc | cc generating | cc monitoring | cc activating | cc deactivating`

The following table explains the elements of the command:

Option	Description
`-e`	Lists the OAM entries.
`-c`	Runs an OAM F5 continuity test.
`-l`	Runs an OAM F5 loopback test.
`-p`	Toggles OAM internal debug messages.
`-L`	Runs an OAM F4 loopback test.
`-C`	Runs an OAM F4 continuity test.
`slot`	Slot number of the LIM.
`port`	Number of the DSL port from which testing cells are sent.
`vpi`	Virtual path identifier (VPI) on which to transmit testing cells.
`vci`	Virtual channel identifier (VPI) on which to transmit testing cells.
`s`	Runs a segment test.
`e`	Runs an end-to-end test.
`cell-count`	Number of F4 loopback cells to send.
`+`	Starts a continuity test.
`-`	Stops a continuity test.
`-q fault normal`	Displays OAM entries with no defects.
`fault ais`	Displays OAM entries with AIS defects.
`fault rdi`	Displays OAM entries with RDI defects.
`fault loc`	Displays OAM entries with LOC defects.

Option	Description
cc generating	Displays OAM entries generating CC cells.
cc monitoring	Displays OAM entries monitoring CC cells.
cc activating	Displays OAM entries in activating state.
cc deactivating	Displays OAM entries in deactivating state.

Overview of the atm-oam profile

Running an OAM test using the atm-oam profile has the following capabilities and limitations:

- An atm-oam profile can be created for testing a single ATM circuit or for testing multiple ATM circuits. When testing multiple circuits using one profile, you can run a loopback test only. One ATM circuit is tested at a time. On each ATM circuit, a specified number of loopback cells are sent, with an interval of 1 second between each transmission. After the test on one circuit is complete, the unit tests the next circuit.
- While testing one ATM circuit using one profile, you can run loopback and continuity tests concurrently.
- Any changes made in an atm-oam profile results in restarting the test. Only that test whose subprofile is changed is restarted.
- If the test is in a waiting stage and you change any of the test parameters, the unit restarts the test using the new parameters.

Following is a sample atm-oam profile and its contents:

```
[in ATM-OAM/{ { any-shelf any-slot 0 } 0 0 } (new)]
oam-address* = { { any-shelf any-slot 0 } 0 0 }
loopback-config = { no segment 1 0 no 1 30 }
continuity-config = { no segment }
```

The oam-address parameter is a complex field that specifies the shelf, slot, port, vpi, and vci values for an ATM interface on which the test is carried out.

- To perform tests on all the ports for the specified slot, specify 0 (zero) for the port value.
- To perform tests for all VPIs on the specified slot and port, specify 32768 for the vpi value.
- To perform tests for all VCIs on the specified slot and port, specify 32768 for the vci value.
- To run an F4 test, specify 32769 for the vci value. To run an F5 test, specify a vci value greater than 31.

Valid oam-address values

You can specify the shelf, slot, port, vpi, and vci values in the following combinations only. All other combinations are invalid.

- shelf=*number*, slot=*number*, port=0, vpi=32768, vci=32769 or vci=32768

This combination causes the unit to test all the VPI-VCI pairs configured on the specified slot. If `vci` is set to 32769, the test is an F4 loopback. Otherwise, the test is an F5 loopback.

- `shelf=`*`number`*, `slot=`*`number`*, `port=`*`number`*, `vpi=32768`, `vci=32769` or `vci=32768`

  This combination causes the unit to test all the VPI-VCI pairs configured on the specified port. If `vci` is set to 32769, the test is an F4 loopback. Otherwise, the test is an F5 loopback.

- `shelf=`*`number`*, `slot=`*`number`*, `port=`*`number`*, `vpi=`*`number`*, `vci=32769`, `32768`, or *`number`*.

If `vci` is set to `32769`, the unit performs an F4 test on its associated VPI. If `vci` is set to `32768`, the unit performs an F5 loopback test on all configured VCIs associated with the specified VPI. If you set `vci` to any other value, the unit performs a loopback or continuity test on the specified VPI-VCI pair.

Settings in the `continuity-config` subprofile

The `continuity-config` subprofile include the following parameters:

Parameter	Setting
`enabled`	Enable/disable continuity checking. Specify `yes` to enable continuity checking or `no` (the default) to disable it. After the specified tests are complete, this parameter is reset by the system to its default.
`continuity-level`	Type of loopback test. Specify `end-to-end` to test at the end-to-end level or `segment` (the default) to test at the segment level.

Settings in the `loopback-config` subprofile

The `loopback-config` subprofile includes the following parameters:

Parameter	Setting
`enabled`	Enable/disable loopback testing. Specify `yes` to enable loopback testing or `no` (the default) to disable. After the specified tests are complete, the system resets this parameter to its default value.
`loopback-level`	Type of loopback test. Specify `end-to-end` to test at the end-to-end level or `segment` (the default) to test at the segment level.
`loopback-cells`	Number of loopback-per-test cells to be sent on each ATM circuit to be tested. Specify a number from 1 (the default) through 10. The time interval between transmission of each loopback cell is 1 second.

Parameter	Setting
`error-threshold`	Threshold for the number of loopback cells that can be lost. If the number of cells lost becomes equal to or greater than this value, a trap is generated. Specify a number from 0 through 10. The default, 0 (zero), disables this trap.
`restart-after-trap`	Enable/disable continuing a test after a trap is generated. Specify `yes` to continue testing after a trap is generated or `no` (the default) for testing to stop after a trap is generated. This parameter has no effect in the case of profiles created for multiple testing. In that case, the test is always restarted.
`total-loopback-tests`	Total number of tests to be performed on this interface. Specify a value from 0 through 10000. The default is 1. A value of 0 (zero) specifies continuous testing. If you specify 0, the statistics indicated by the `testCompleted` MIB variable are always 0.
`test-iteration-interval`	Time period in minutes between two tests. Specify a value from 0 through 10000. The default is 30.

You cannot stop a loopback test on an ATM circuit until all configured cells are sent on that circuit. Therefore, you cannot restart the test until the current test on that circuit is complete. If you try to restart the test, the loopback fault status is set to `test already running` and `enabled` is set to `no` in the `loopback-config` subprofile.

F4 OAM support on a VP-switching VPI

You can enable and disable F4 OAM support on each VC-switching VPI.

The indexed parameter `vc-oamf4-support` in the *xxx*`-ATM/{ shelf-1 trunk-module-1 1 }:line-config` subprofile of trunk interfaces controls the enabling and disabling of F4 segment (VCI = 3) and end-to-end (VCI = 4) processing. The `vc-oamf4-support` parameter has a one-to-one mapping with `vc-switching-vpi` parameter.

Following is a sample listing of the relevant parameters in a `line-config` subprofile of an `oc3-atm` trunk profile:

```
[in OC3-ATM/{ shelf-1 trunk-module-1 1 }:line-config]
...
vpi-vci-range = vpi-0-255-vci-32-8191
vc-switching-vpi = [ 1 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 +
vc-oamf4-support = [ yes yes yes yes yes yes yes yes yes yes yes yes yes yes yes+
...
```

Following is the parameter description for `vc-oamf4-support`:

Parameter	Description
`vc-oamf4-support` *N*	Enables/disables specific F4 segment and end-to-end OAM processing on a Stinger VC-switching VPI. With the default `yes` setting, F4 segment and end-to-end processing for the specified VC-switching VPI is enabled. To disable F4 segment and end-to-end processing for the VC-switching VPI, specify .

By default, the `vc-oamf4-support` parameter is enabled for all VC-switching VPIs, including all of the default `vc-switching-vpi = 0` elements.

To disable the F4 OAM support for the 0 VPI, you must disable all the corresponding `vc-oamf4-support` parameter entries that have a `0` entry in the `vc-switching-vpi` parameter. You must repeat the preceding process for each trunk for which you would like to disable F4 OAM processing.

Continuity check and monitoring

F4 and F5 OAM continuity tests can be initiated as follows:

- Locally, using the command-line interface (CLI).
- Remotely, a network peer can send activation/deactivation requests to initiate a continuity test.

You can start an OAM continuity test locally using the command-line interface by using the `oam -c|C +` command or by setting the parameters in the `atm-oam` profile. Locally initiated continuity tests only configure the Stinger system to generate continuity cells. For both continuity check and OAM defects, events are reported by way of SNMP traps.

Continuity checks started by a remote peer are not associated with the command-line interface or a profile. For both continuity check and OAM defects, events are reported via SNMP traps.

Continuity check implementation

Stinger systems implement the standard OAM continuity check protocol. Note, however, that any remote deactivate request is accepted by the Stinger unit regardless of the direction indicated by remote peer. A remote activate request is accepted only if its specified directions is compatible with local settings (see “While in the default direction state, what happens when a Stinger unit receives an activation request” on page 8-8 for details).

When a connection is created, the OAM flow(s) associated with a connection have their continuity check direction set to *default*. The default direction indicates that the system generates no continuity check cells and does not monitor continuity check cells. The system also does not send any activation or deactivation requests to the remote.

Stinger systems support the generation of continuity cells towards the remote peer. When you start a test using the `oam` command or the `atm-oam` profile, from the perspective of the Stinger unit, the generation of continuity cells towards the remote peer is in the A-to-B direction. The A-to-B direction means that the Stinger unit

sends an activate request to the remote peer. Stopping the test resets the direction to default.

While in the default direction state, what happens when a Stinger unit receives an activation request

When a Stinger unit is in the default direction and a remote peer sends a continuity check activate request, the Stinger unit accepts any direction that the remote peer specifies. The default direction is compatible with any direction sent by the peer. The A-to-B direction is only compatible when the B-to-A direction is specified by the remote peer.

Table 8-1 lists the possible directions that the remote peer can specify and the resulting action that the Stinger takes.

Table 8-1. Continuity check direction specified by the remote peer and the results

Remote request direction	Result
A-to-B	From the Stinger perspective, the B-to-A direction. The network peer generates the continuity check cells. The Stinger unit monitors continuity check cells.
B-to-A	From the perspective of the Stinger unit, the A-to-B direction. Stinger unit generates continuity check cells to the network peer.
2-way	Stinger unit monitors the continuity check cells generated by the network peer. Stinger unit generates continuity check cells to the network peer.

What happens when you start a continuity check locally

When you start a continuity check test using the `oam` command or the `atm-oam` profile, the continuity check direction is set to A-to-B (Stinger generates continuity check cells to the network peer). While the continuity check is set to A-to-B direction, the Stinger unit accepts activate requests from the remote peer only if the direction specified by the remote peer is B-to-A. The Stinger direction stays in the A-to-B direction until you deactivate the test locally using the `oam` command or the `atm-oam` profile, at which point the direction reverts to default.

Deactivating a continuity check test

The continuity check remains active until one of the following events occurs:

- You delete the cross connection.
- The Stinger unit receives a request to deactivate the continuity check either locally or from the remote. Consider the following situations:
  - If you start a test by setting parameters in the `atm-oam` profile, you can stop the test only by setting the appropriate parameters in that profile.
  - If you start a continuity check using the `oam -c|C +` command, you can stop the test only by using the `oam -c|C -` command.

– If a test was started by a network peer, the network peer can send a deactivate request. You can also stop the test can by using the `oam -c|C -` command or by setting parameters in the `atm-oam` profile.

Running F4 and F5 continuity tests using the `oam` command

To run a continuity test from a control module, use the following syntax:

`oam -C` *`slot port vpi`* `|-c` *`slot port vpi`* `[`*`vci`*`] e|s +|-`

You can also run a continuity test from a LIM by first opening a session with the LIM. When you run a continuity test from a LIM, the *slot* option no longer applies.

The `oam - c | C +` command starts a continuity check and `oam -c | C` stops the continuity check on an F5 (`oam -c`) or F4 (`oam -C`) flow. When the continuity test is started, the continuity check direction is set to A-to-B (the Stinger generates continuity check cells to the remote peer). When the test is stopped, the continuity check direction is reset to default.

The following sample command entered on the control module starts a segment continuity check test on port 18, slot 2, VPI 0, VCI 100:

```
admin> oam -c 18 2 0 100 s +
Sending OAM continuity activation cell
```

Note that the continuity check direction for this continuity check is now set to A-to-B (Stinger unit to the remote peer), and remains in the A-to-B direction until you stop the test using the `oam` command, as in the example below:

```
admin> oam -c 18 2 0 100 s -
Sending OAM continuity deactivation cell
```

Note that the continuity check direction for this continuity check is now set to default.

The following sample command entered on the control module starts an end-to-end continuity check test on port 17, slot 2, VPI 0:

```
admin> oam -C 17 2 0 e +
Sending F4 OAM continuity activation cell
```

The following command stops the preceding test:

```
admin> oam -C 17 2 0 e -
Sending F4 OAM continuity deactivation cell
```

The following sample command entered on the control module starts an F5 end-to-end continuity check test on port 17, slot 2, vpi 0, vci 35:

```
admin> oam -c 17 2 0 35 e +
```

The following command stops the preceding test:

```
admin> oam -c 17 2 0 35 e -
```

The following sample command entered on the control module starts an F5 end-to-end continuity check test on port 17, slot 2, VPI 0, VCI 35:

```
admin> oam -C 17 2 0 35 e +
```

The following command stops the preceding test:

```
admin> oam -C 17 2 0 35 e -
```

To instruct the Stinger unit to perform an F5 segment continuity test from a T1000 module in slot 3, over VCI 36, proceed as follows:

```
admin> open 1 3

t1000-1/3> oam -c 3 0 36 s +
Sending OAM continuity activation cell
```

The following command stops the preceding test:

```
t1000-1-1/3> oam -c 3 0 36 s -
Sending OAM continuity deactivation cell
```

Running F5 continuity tests using the atm-oam profile

The following sample commands start an F5 continuity check on slot 15, port 2, VPI 3 and VCI 40:

```
admin> new atm-oam {{ 1 15 2} 3 40}
ATM-OAM/{{ 1 15 2} 3 40} read

admin> set continuity-config enabled = yes

admin> set continuity-config continuity-level = end-to-end

admin> write
ATM-OAM/{{ 1 15 2} 3 40} written
```

To disable the preceding continuity check, enter the following commands:

```
admin> new atm-oam {{ 1 15 2} 3 40}
ATM-OAM/{{ 1 15 2} 3 40} read

admin> set continuity-config enabled = no

admin> write
ATM-OAM/{{ 1 15 2} 3 40} written
```

OAM loopback tests

You run can use the `oam -Ll` command or set the parameters in the `atm-oam` profile and its `loopback-config` subprofile to run an F4 or F5 OAM loopback test.

Running F4 and F5 loopback tests using the oam command

To run a loopback test from the control module, use the following syntax:

oam -L *slot port vpi*|-l *slot port vpi* [*vci*] e|s *cell-count*

You can also run a loopback test from a LIM by first opening a session with the LIM. When you run a loopback test from a LIM, the *slot* option no longer applies.

For example, to send 64 consecutive segment OAM F4 loopback cells to VPI 15 on DSL port 2, issue the following command from a trunk module or LIM:

```
admin> oam -L 2 15 s 64
```

To display additional information about the outgoing and incoming segment test cells, use the following command:

```
admin> oam -p
```

The following sample command runs an end-to-end F4 loopback test by sending one cell over VPI 1, port 1 in slot 18 from the control module:

```
admin> oam -L 18 1 1 e 1
Received our F4 OAM end-to-end loopback cell, Id=0
```

The following sample commands run an F5 OAM segment loopback test from a Stinger MRT unit to the CPE connected to it on port 12.

```
admin> open 1 1

mrtdmt-1/1> oam -e
OAM Entry list
Entry=3f0ca0, Linear Port=12 vpi=8, vci=3 state=Up loopTx=0 loopRx=0
Segment Continuity=READY  End2End Continuity=READY isVpc=No
Entry=3f0de0, Linear Port=12 vpi=8, vci=4 state=Up loopTx=0 loopRx=0
Segment Continuity=READY  End2End Continuity=READY isVpc=No
Entry=3f0b60, Linear Port=12 vpi=8, vci=35 state=Up loopTx=0 loopRx=0
Segment Continuity=READY  End2End Continuity=READY isVpc=No
Entry=47e620, Linear Port=24 vpi=8, vci=3 state=Up loopTx=0 loopRx=0
Segment Continuity=READY  End2End Continuity=READY isVpc=No
Entry=47e760, Linear Port=24 vpi=8, vci=4 state=Up loopTx=0 loopRx=0
Segment Continuity=READY  End2End Continuity=READY isVpc=No
Entry=47e4e0, Linear Port=24 vpi=8, vci=35 state=Up loopTx=0 loopRx=0Segment
Continuity=READY  End2End Continuity=READY isVpc=No

mrtdmt-1/1> oam -l 12 8 35 s 1
mrtdmt-1/1> Sending F5 OAM segment loopback cell, Id=0
Received our F5 OAM segment loopback cell, Id=0
OAM: received our F5 OAM segment loopback #0
```

The following sample commands run an F5 OAM segment loopback test from the SHDSL/HDSL2 LIM in slot 4 of a Stinger unit to the CPE connected to port 25 of the LIM.

```
admin> open 1 4

hdsl2-1/4> oam -e
OAM Entry list
Entry=4743e0, Linear Port=25 vpi=0, vci=3 state=Up loopTx=0 loopRx=0
Segment Continuity=READY  End2End Continuity=READY isVpc=No
Entry=474520, Linear Port=25 vpi=0, vci=4 state=Up loopTx=0 loopRx=0
Segment Continuity=READY  End2End Continuity=READY isVpc=No
Entry=473f60, Linear Port=25 vpi=0, vci=35 state=Up loopTx=0 loopRx=0
Segment Continuity=READY  End2End Continuity=READY isVpc=No
Entry=475da0, Linear Port=26 vpi=0, vci=3 state=Up loopTx=0 loopRx=0
Segment Continuity=READY  End2End Continuity=READY isVpc=No
Entry=477760, Linear Port=26 vpi=0, vci=4 state=Up loopTx=0 loopRx=0
Segment Continuity=READY  End2End Continuity=READY isVpc=No
Entry=475c60, Linear Port=26 vpi=0, vci=35 state=Up loopTx=0 loopRx=0
Segment Continuity=READY  End2End Continuity=READY isVpc=No
Entry=4779e0, Linear Port=27 vpi=0, vci=3 state=Up loopTx=0 loopRx=0
Segment Continuity=READY  End2End Continuity=READY isVpc=No
Entry=477b20, Linear Port=27 vpi=0, vci=4 state=Up loopTx=0 loopRx=0
Segment Continuity=READY  End2End Continuity=READY isVpc=No
Entry=4778a0, Linear Port=27 vpi=0, vci=35 state=Up loopTx=0 loopRx=0
Segment Continuity=READY  End2End Continuity=READY isVpc=No
Entry=478ea0, Linear Port=28 vpi=0, vci=3 state=Up loopTx=0 loopRx=0
Segment Continuity=READY  End2End Continuity=READY isVpc=No
Entry=478fe0, Linear Port=28 vpi=0, vci=4 state=Up loopTx=0 loopRx=0
```

```
Segment Continuity=READY  End2End Continuity=READY isVpc=No
Entry=478d60, Linear Port=28 vpi=0, vci=35 state=Up loopTx=0 loopRx=0
Segment Continuity=READY  End2End Continuity=READY isVpc=No
hdsl2-1/4> oam -l 25 0 35 s 1
hdsl2-1/4> Sending F5 OAM segment loopback cell, Id=0
Received our F5 OAM segment loopback cell, Id=0
OAM: received our F5 OAM segment loopback #0
```

Running F4 and F5 loopback tests using the atm-oam profile

To run an F4 or F5 loopback test, you set the parameters in the loopback-config subprofile. You can test multiple ATM circuits using a single atm-oam profile.

Sample F4 OAM loopback test

The following sample commands configure four end-to-end, F4 loopback tests on slot 10, port 1, VPI 2, with a time interval of 30 minutes between each test and two cells per test:

```
admin> new atm-oam {{ 1 10 1} 2 32769}
ATM-OAM/{{ 1 10 1} 2 32769} read
admin> set loopback-config enabled = yes
admin> set loopback-config loopback-level = end-to-end
admin> set loopback-config loopback-cells-per-test = 2
admin> set loopback-config total-loopback-tests = 4
admin> write
ATM-OAM/{{ 1 10 1} 2 32769} written
```

Sample F5 OAM loopback test

The following sample commands configure four end-to-end, F5 loopback tests on slot 10, port 1, VPI 2, and VCI 35 with a time interval of 30 minutes between each test and two cells per test:

```
admin> new atm-oam {{ 1 10 1} 2 35}
ATM-OAM/{{ 1 10 1} 2 35} read
admin> set loopback-config enabled = yes
admin> set loopback-config loopback-level = end-to-end
admin> set loopback-config loopback-cells-per-test = 2
admin> set loopback-config total-loopback-tests = 4
admin> set loopback-config test-iteration-interval = 30
admin> write
ATM-OAM/{{ 1 10 1} 2 35} written
```

Testing multiple ATM circuits

The following examples illustrate how multiple ATM circuits can be tested by means of a single profile. Assume that the shelf value is 1 and the slot value is 15.

- To perform an F4 test on all VPIs on port 2, enter the following at the command-line interface:

```
admin> new atm-oam {{ 1 15 2} 32768 32769}
ATM-OAM/{{ 1 15 2} 32768 32769} read

admin> write
ATM-OAM/{{ 1 15 2} 32768 32769} written
```

Then, when you configure the `loopback-config` subprofile, the test is run on all the ATM circuits configured for the port.

- To perform an F4 test on all VPIs for all ports on slot 15, enter the following at the command-line interface:

```
admin> new atm-oam {{ 1 15 0} 32768 32769}
ATM-OAM/{{ 1 15 0} 32768 32769} read

admin> write
ATM-OAM/{{ 1 15 0} 32768 32769} written
```

Then, when you configure the `loopback-config` subprofile, the test is run on all the ATM circuits on slot 15.

- To perform an F5 test on all VCIs with VPI 3 on port 2 of slot 15, enter the following at the command-line interface:

```
admin> new atm-oam {{ 1 15 2} 3 32768}
ATM-OAM/{{ 1 15 2} 3 32768} read

admin> write
ATM-OAM/{{ 1 15 2} 3 32768} written
```

Then, when you configure the `loopback-config` subprofile, the test is run on port 2 of slot 15 for all ATM circuits with VPI 3.

- To perform an F5 test on all configured VPI-VCI pairs on port 2, enter the following at the command-line interface:

```
admin> new atm-oam {{ 1 15 2} 32768 32768}
ATM-OAM/{{ 1 15 2} 32768 32768} read

admin> write
ATM-OAM/{{ 1 15 2} 32768 32768} written
```

- To perform an F5 test on all VPI-VCI pairs for all ports on slot 15, enter the following at the command-line interface:

```
admin> new atm-oam {{ 1 15 0} 32768 32768}
ATM-OAM/{{ 1 15 0} 32768 32768} read

admin> write
ATM-OAM/{{ 1 15 0} 32768 32768} written
```

Then, when you configure the `loopback-config` subprofile, the test is run on all VPI-VCI pairs on slot 15.

Specifying that a trap is sent

The `error-threshold` parameter in the `loopback-config` subprofile enables the Stinger unit to generate a trap when the number of lost cells is greater than or equal to a specified threshold value. For example:

```
admin> set loopback-config error-threshold = 1
```

The `oam-timeout-trap-enabled` parameter in the `trap` profile enables and disables an OAM timeout trap and the `error-threshold` parameter. To enable the trap, specify `yes`. To disable the trap (the default), specify `no`.

Using the `oamloop` command

The `oamloop` command sends ATM OAM loopback cells on an ATM interface, to obtain information about the results of the looped cells.

Note Running several prolonged concurrent OAM test sessions using the `oamloop` command sometimes causes inaccurate test results. To prevent this situation, Lucent Technologies strongly recommends that you conduct only one OAM test session at a time using this software version. If you must conduct simultaneous OAM test sessions, limit them to no more than eight. Additionally, avoid running the test unnecessarily for prolonged periods.

You enter the `oamloop` command with options to specify the type of cells to transmit, the shelf number (always 1), the slot where the trunk module is located, and the virtual path identifier (VPI) and virtual channel identifier (VCI) on which to send the cells. You can optionally specify the number of cells and the transmission interval. For details about `oamloop` syntax, see the *Stinger Reference*.

For example, the following command sends 10 end-to-end loopback cells to a trunk module in slot 2 on VPI 1, VCI 32:

```
admin> oamloop -c 10 -e 1 2 1 32
Received our End2End OAM loopback cell, Id=9
Received our End2End OAM loopback cell, Id=10
Received our End2End OAM loopback cell, Id=11
Received our End2End OAM loopback cell, Id=12
Received our End2End OAM loopback cell, Id=13
Received our End2End OAM loopback cell, Id=14
Received our End2End OAM loopback cell, Id=15
Received our End2End OAM loopback cell, Id=16
Received our End2End OAM loopback cell, Id=17
Received our End2End OAM loopback cell, Id=18
--- OAM loop statistics ---
10 cells transmitted, 10 cells received, 0% cell loss
```

Configuring loopback on OC3, E3, and DS3 interfaces

To run a loopback test on the interface of an OC3-ATM, E3-ATM, or DS3-ATM trunk module, set the `loopback` parameter in the `line-config` subprofile of the `oc3-atm`, `ds3-atm`, or `e3-atm` profile. While the interface is looped back, normal data traffic is interrupted.

Specify one of the following values for the `loopback` parameter:

- `no-loopback` (the default)—The line is operating normally and is not running loopback testing.
- `facility-loopback`—This line is put in loopback mode, and the trunk module returns the signal it receives on its line.
- `local-loopback`—This line is put in loopback mode, and the trunk receive path is connected to the transmit path at the multiplexer. The transmitted signal is still sent to the network as well.

The procedure for running a loopback test on the OC3-ATM, DS3-ATM, and E3-ATM trunk modules are similar. For more information, see the module configuration guide for your device. The following sample commands activate a local loopback on an OC3-ATM trunk line:

```
admin> read oc3-atm {1 17 1}
OC3-ATM/{ shelf-1 slot-17 1 } read

admin> list line-config
[in OC3-ATM/{ shelf-1 trunk-module-1 1 }:line-config]

admin> set loopback = local-loopback

admin> write
OC3-ATM/{ shelf-1 trunk-module-1 1 } written
```

To stop the loopback, proceed as follows:

```
admin> set line loopback = no-loopback

admin> write
OC3-ATM/{ shelf-1 trunk-module-1 1 } written
```

The `oc3-atm-stat`, `ds3-atm-stat`, and `e3-atm-stat` profiles display the status of the trunk lines. For an explanation about the parameters in these profiles, see the module configuration guide for your device or the *Stinger Reference*.

Displaying OAM entries

You can use the oam -e and oam -q commands enable you to display OAM entries in a Stinger system.

The `oam -e` command displays details about OAM entries that exist in the system. You can display OAM entries, for a specific slot, port, VPI, or VCI. The `oam -e` command reports a large number of OAM entries. The `oam -q` command enables you to display subsets of the OAM entries reported by the `oam -e` command.

The output of these commands reports the following information:

Element	Indicates
OAM test information	This information is reported in the following sample format: `F4-SEG (8373e890:3507.1.3)`. In this sample output, the first group of characters indicate whether the test is an F4 or F5 test and whether the test is a segment or end-to-end test. The next group of characters (preceding the colon), `8373e890`, is not for administrative use. The second group of numbers (after the colon), `3507`, is the internal trunk identification number. The last set of numbers, `1.3`, represents the VPI and VCI values.
`E2E`	Applicable only for F5 OAM entries. Whether an end point is a segment (`FALSE`) or end-to-end point (`TRUE`).
`loop`	Number of transmitted (`Tx`) and received (`Rx`) loopback cells.

Element		Indicates
F		Fault state. Possible fault states are: ■ NORMAL—No faults are detected. ■ AIS—an alarm indication signal cell is received. ■ RDI—a remote defect indication (RDI) cell is received. ■ LOC—loss of continuity. An LOC condition is detected when the system is monitoring continuity check cells and no cells are received for a specified time period.
CC		Continuity check information.
	G	Continuity check cell generation state. Possible states are stopped and activate.
	R	Entity that requested the continuity check activation. Possible values are: ■ NONE—the continuity check is stopped or is active as a result of an activation request from the network peer. ■ CLI—the continuity check was initiated using the oam -c|C command. ■ PROF—the continuity check was initiated by setting parameters in the atm-oam profile.
	M	Continuity check monitoring state. Possible states are stopped, normal, and LOC.
	A	Continuity check activation/deactivation state. Possible states are ready, active, activating (ACTG), and deactivating (DEACTG).
D		Continuity check direction
	P	Provisioned direction—The direction supported by the flow. It can be either default or A-to-B. When the flow is first created it is set to default. It is set to A-B and reset to default when you use the oam -c|C command or the atm-oam profile
	C	Current direction is the actual direction (from Stinger unit's perspective) of the OAM flow. Note that when a network peer has initiated a continuity check test, that Stinger unit's perspective is the inverse. That is, when the network is A-B (generating), Stinger is B-A (monitoring) and vice versa.

Using the oam -e command

The syntax of the oam -e command is as follows:

oam -e [***slot***] [***port***] [***vpi***] [***vci***]|**-p**

Following is an example of an F4 segment flow. The number of transmitted loopback cells is 0 and the number of received (Rx) loopback cells is 0. The fault state is normal (no fault). Continuity cell generation is stopped, monitoring for continuity cells is stopped, and the continuity check activating state is ready (not active). The provisioned direction is set to default and the current direction is also default.

```
F4-SEG(8373e890:3507.1.3) loop(Tx=0, Rx=0)
```

```
  8373e890:F=NORMAL CC(R=NONE:G=STOP M=STOP A=READY D(P=DEF C=DEF))
```

Following is an example of an F4 end-to-end output:

```
F4-E2E(8373eaa0:3507.1.4) loop(Tx=0, Rx=0)
  8373eaa0:F=NORMAL CC(R=NONE:G=STOP M=STOP A=READY D(P=DEF C=DEF))
```

Following is an example of an F5 terminating connection output. It has both segment and end-to-end flows. The `SEG` line represents the segment flow and the `E2E` line represents the end-to-end flow.

```
F5(8373e6b0:3507.1.102) E2E=TRUE loop(Tx=0, Rx=0)
  SEG:8373e6b0:F=NORMAL CC(R=NONE:G=STOP M=STOP A=READY:D(P=DEF C=DEF))
  E2E:8373e6b0:F=NORMAL CC(R=NONE:G=STOP M=STOP A=READY:D(P=DEF C=DEF))
```

Using the `oam -q` command

You can use the `oam -q` command with the following arguments:

Argument	Displays
`fault normal`	OAM entries with no defects.
`fault ais`	OAM entries with AIS defects.
`fault rdi`	OAM entries with RDI defects.
`fault loc`	OAM entries with LOC defects.
`cc generating`	OAM entries generating CC cells.
`cc monitoring`	OAM entries monitoring CC cells.
`cc activating`	OAM entries in activating state.
`cc deactivating`	OAM entries in deactivating state.

Displaying entries with no defects

To display entries with no defects, use the `oam -q fault normal` command. For example:

```
admin> oam -q fault normal
OAM Entry list
F: fault state
CC: continuity information
R: Continuity requester
G: CC generation state
M: CC monitoring state
A: CC Activation/Deactivation state
D: Direction. P: provisioned direction. C: current direction

F4-SEG(836ebc10:2.0.3) loop(Tx=0, Rx=0)
   836ebc10:F=NORMAL CC(R=NONE:G=STOP M=STOP A=READY D(P=DEF C=DEF))

F4-E2E(836d0ac0:2.0.4) loop(Tx=0, Rx=0)
   836d0ac0:F=NORMAL CC(R=NONE:G=STOP M=STOP A=READY D(P=DEF C=DEF))

F5(82048320:3505.0.100) E2E=FALSE loop(Tx=0, Rx=0)
```

```
   SEG:82048320:F=LOC CC(R=NONE:G=ACTIVE M=LOC A=ACTIVE:D(P=DEF C=2WAY))

Total matching Oam Channels=3
```

Displaying AIS defects

To display entries with AIS defects, use the `oam -q fault AIS` command. For example:

```
admin> oam -q fault ais
OAM Entry list
F: fault state
CC: continuity information
R: Continuity requester
G: CC generation state
M: CC monitoring state
A: CC Activation/Deactivation state
D: Direction. P: provisioned direction. C: current direction

F4-SEG(836998a0:3505.0.3) loop(Tx=0, Rx=0)
   836998a0:F=AIS CC(R=NONE:G=STOP M=STOP A=READY D(P=DEF C=DEF))

Total matching Oam Channels=1
```

Displaying RDI defects

To display entries with RDI defects, use the `oam -q fault RDI` command. For example:

```
admin> oam -q fault rdi
OAM Entry list
F: fault state
CC: continuity information
R: Continuity requester
G: CC generation state
M: CC monitoring state
A: CC Activation/Deactivation state
D: Direction. P: provisioned direction. C: current direction

F4-E2E(836999e0:3505.0.4) loop(Tx=0, Rx=0)
   836999e0:F=RDI CC(R=NONE:G=STOP M=STOP A=READY D(P=DEF C=DEF))
Total matching Oam Channels=1
```

Displaying LOC defects

To display entries with LOC defects, use the `oam -q fault loc` command. For example:

```
admin> oam -q fault loc
OAM Entry list
F: fault state
CC: continuity information
R: Continuity requester
G: CC generation state
```

```
M: CC monitoring state
A: CC Activation/Deactivation state
D: Direction. P: provisioned direction. C: current direction

F5(82048320:3505.0.100) E2E=FALSE loop(Tx=0, Rx=0)
   SEG:82048320:F=LOC CC(R=NONE:G=ACTIVE M=LOC A=ACTIVE:D(P=DEF C=2WAY))
```

Displaying continuity check cell generation

To display OAM entries generating continuity cells, use the `oam -q cc generating` command. For example:

```
admin> oam -q cc generating
Matching OAM Entry List
F: fault state
CC: continuity information
R: Continuity requester
G: CC generation state
M: CC monitoring state
A: CC Activation/Deactivation state
D: Direction. P: provisioned direction. C: current direction

F5(82048320:3505.0.100) E2E=FALSE loop(Tx=0, Rx=0)
   SEG:82048320:F=LOC CC(R=NONE:G=ACTIVE M=LOC A=ACTIVE:D(P=DEF C=2WAY))

Total matching Oam Channels=1
```

Displaying OAM entries for monitoring continuity check cells

To display OAM entries for monitoring CC cells, use the `oam -q cc monitoring` command. For example:

```
admin> oam -q cc monitoring
    Matching OAM Entry List
    F: fault state
    CC: continuity information
    R: Continuity requester
    G: CC generation state
    M: CC monitoring state
    A: CC Activation/Deactivation state
    D: Direction. P: provisioned direction. C: current direction

    F5(82048320:3505.0.100) E2E=FALSE loop(Tx=0, Rx=0)
       SEG:82048320:F=LOC CC(R=NONE:G=ACTIVE M=LOC A=ACTIVE:D(P=DEF C=2WAY))


   Total matching Oam Channels=1
```

Fault reporting and alarms

Stinger systems use SNMP traps to report OAM changes for an OAM end point. Stinger systems implement the standard OAM fault protocol, with the exception that data cells and loopback cells do not clear alarms.

Fault and defect conditions and continuity check activation and deactivation events are reported through alarms.

The following conditions are detected and reported by the system:

- RDI defect raise/clear
- LOC defect raise/clear
- AIS defect raise/clear
- NONE clear any of the above defects, clear most recent raised defect. When raised, it indicates that the endpoint flow does not have any defects.

These following events related to continuity check activation and deactivation are reported through alarms:

- CC-ACTIVE indicates that continuity check has activated successfully
- CC-READY indicates that continuity check is in ready/inactive state
- CC-RX-DENIED indicates that a NAK was received from the peer
- CC-TX-DENIED indicates that we sent a NAK to the peer
- CC-ACT-TIMEOUT indicates that the activation request timed out
- CC-DEACT-TIMEOUT indicates that the deactivation request timed out

Traps for AIS/RDI and continuity check alarms

To configure the Stinger unit to send following OAM traps for defect and continuity check events, set the `oam-timeout-trap-enabled` in the `trap` profile is set to `yes`:

Trap	Description
`atmOamDefectSegTrap`	Segment OAM Defect. Used to send a trap when a segment flow reports an AIS, LOC, or RDI defect.
`atmOamDefectE2eTrap`	End-to-end OAM Defect. Used to send a trap when an end point flow reports an AIS, LOC, or RDI defect.

Internal and external diagnostic tests

You can use an internal diagnostic test (IDT) to identify problems that might occur during data transfer between the control module and LIMs. If you activate an IDT for a line, the control module generates a data stream internally and sends it to that line. The line loops back the data to the control module. The control module then analyzes the data and reports the statistics in the `line-diag-stat` profile. (You can also use SNMP to perform internal diagnostic testing. For additional information, see the *Stinger TAOS 9.1-142 Cumulative Release Note.)*

The external diagnostic test (EDT) feature puts the DSL modem into loopback mode. If a complete circuit is established, you can then send a data stream from an external device (such as a network traffic generator) through the trunk to the modem. The modem loops back the data stream to the external device, where it can be analyzed.

Running an internal diagnostic test (IDT)

The Stinger unit creates a `line-diag` profile for each interface or port, which you use to run internal diagnostic tests and bit-error rate tests (BERTs). You use the

idt-enable and idt-num-of-msg parameters in the line-diag profile to run an internal diagnostic test. The system also creates a read-only line-diag-stat profile, which shows the status and statistics for these diagnostic tests.

The Stinger unit also supports external diagnostic testing (see "Running an external diagnostic test (EDT) feature" on page 8-22). The loopback type for running internal diagnostic tests is digital and is not affected by the loopback type configured for external diagnostic testing.

Following are the parameters in the line-diag and line-diag-stat profiles that relate to internal diagnostic testing. The parameters are shown here with default values:

```
[in LINE-DIAG/{ shelf-1 slot-12 1 }]
idt-enable = no
idt-num-of-msg = 1000
```

```
[in LINE-DIAG-STAT/{ shelf-1 slot-12 1 }]
idt-operation-state = stopped
idt-send-count = 0
idt-recv-count = 0
idt-error-counter = 0
```

Parameter	Setting
idt-enable	Enable/disable internal diagnostic testing on the line. Specify yes to enables internal diagnostic testing on the line or no (default) to disable it.
idt-num-of-msg	Number of messages that the control module sends to the line. Each message corresponds to four ATM cells. The data payload of each message consists of sequential numeric data. By default, the value of this parameter is set to 1000. Enter a value from 0 through 10000.
idt-operation-state	Status of an internal diagnostic test on the line. (This parameter is read-only.) By default, this parameter shows stopped (the test is inactive). When the line is undergoing internal diagnostic testing, this parameter shows active.
idt-send-count	Number of messages sent from the LIM to the control module. (This parameter is read-only.)
idt-recv-count	Number of messages received by the control module. (This parameter is read-only.)
idt-error-counter	Number of erroneous messages received by the control module. (This parameter is read-only.)

The following sample commands instruct the Stinger unit to run an internal diagnostic test on port 1 of slot 2:

```
admin> read line-diag {1 2 1}
LINE-DIAG/{ shelf-1 slot-2 1 } read
```

```
admin> list
[in LINE-DIAG/{ shelf-1 slot-2 1 }]
```

```
admin> set idt-enable = yes
```

```
admin> set idt-num-of-msg = 1000
```

```
admin> write
```

To view the results of the internal diagnostic test, display the contents of the `line-diag-stat` profile, as shown in the following example:

```
admin> read line-diag-stat {1 2 1}
LINE-DIAG-STAT/{ shelf-1 slot-2 1 } read

admin> list
[in LINE-DIAG-STAT/{ shelf-1 slot-2 1 }]
physical-address* = { shelf-1 slot-2 1 }
bert-operation-state = stopped
idt-operation-state = stopped
bert-error-counter = 0
idt-send-count = 1000
idt-recv-count = 1000
idt-error-counter = 0
```

If you attempt to modify the `idt-enable` parameter while an internal diagnostic test is active for a line, the system generates a warning message as follows:

```
admin> set idt-enable = no

admin> write
LOG warning, Shelf 1, Controller-1, Time: 20:12:30--
IDT Test for {1 3 1} is running !
LINE-DIAG/{ shelf-1 slot-3 1 } written
```

Running an external diagnostic test (EDT) feature

You configure a line for external diagnostic testing by putting it loopback mode. The `loop-back` parameter in the line-config subprofile for a line enables external diagnostic testing.

```
[in HDSL2/{ shelf-1 slot-2 1 }:line-config]
loop-back = none
```

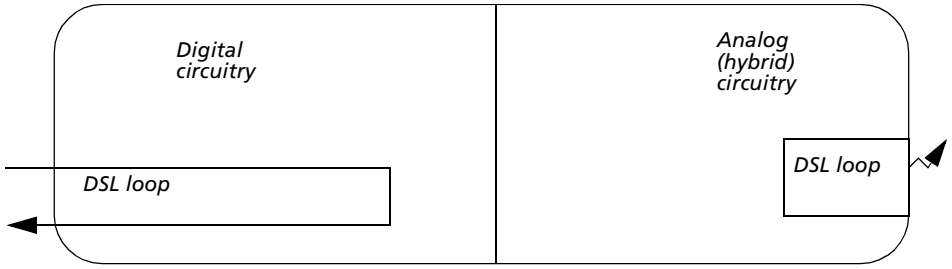
Parameter	Setting
`loop-back`	Whether the line passes normal data or is in loopback mode. Specify one of the following values: ■ `none` (default)—The line is not used for loopback testing and passes normal data. ■ `analog`—The line is enabled for analog loopback testing. (You might need to terminate the DSL line with a 150-ohm resistor.) ■ `digital`—The line is enabled for digital loopback testing.

Note External diagnostic tests in analog mode do not work for the 24-port ADSL LIM if a CPE device is connected and trained up. External diagnostic testing does work in either digital mode or analog mode if no CPE device is attached.

Digital loopback

When a line is enabled for digital loopback, data is looped only at the digital circuitry of the modem. Data does not reach the analog circuitry, as shown in Figure 8-1.

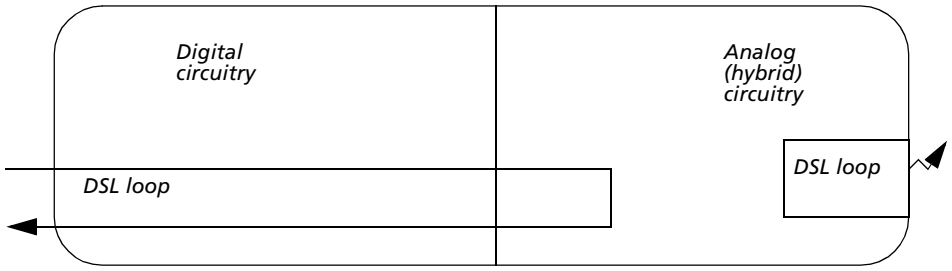
Figure 8-1. Data passes through a modem's digital circuitry (digital loopback).



Analog loopback

When the line is enabled for analog loopback, the data passes from the digital circuitry to analog circuitry and is then looped back, as shown in Figure 8-2. Analog loopback tests more circuitry.

Figure 8-2. Data passes through a modem's digital circuitry and analog circuitry (analog loopback).



The following sample commands put a line into analog loopback mode:

```
admin> read hdsl2 {1 1 1}
HDSL2/{ shelf-1 slot-1 1 } read
admin> set loop-back = analog
admin> write
```

Relay alarm testing

You can use the debug-level `inputrelaytest` command to simulate the status of relays to generate relay alarm and trap conditions for testing.

When you use the `inputrelaytest` command, actual alarms on the system associated with relays are overwritten by this command and are not restored until you reset the system. The actual relay alarm functions revert to normal operation when you disable the test.

Overview of the `inputrelaytest` command

The command-line interface help information for the `inputrelay` command provides syntax information, as shown below:

```
admin> inputrelaytest -h
```

```
   Usage: inputrelaytest [ -p | -i |  -m | -(0-7) | -t | -s -h]
   -p : Toggle poll test/external input relay
   -i : Initialize the test
   -m : Toggle test input relay open/close mode
   -(0-7) : Set test input relay status (0=all)
   -t : Show test input relay status
   -s : Show external input relay status
   -h : help message
During the test, the system generates a warning log message every minute.
LOG warning, Shelf 1, Controller-1, Time: 10:16:58--
  In Test mode! Run "inputrelaytest -p" to set back to external input relay
alarm mode
LOG warning, Shelf 1, Controller-1, Time: 10:18:00--
  In Test mode! Run "inputrelaytest -p" to set back to external input relay
alarm mode
```

Argument	Description
`-p`	Enables/disables the input relay alarm test. When you have completed the test, you must enter the `inputrelaytest -p` command again to return to external input relay alarm mode.
`-i`	Reinitializes the test.
`-m`	Toggles the close or open setting when you set an individual relay.
`-0`	Specifies that all relays are used for testing.
`-1 through -7`	Specifies an individual for testing.
`-t`	Shows the simulation test input relay status.
`-s`	Shows the external input relay status.

Examples using the `inputrelaytest` command

The following sample configure an `alarm` profile, configure a `trap` profile, and runs an input relay test.

The following commands configure the unit to generate an alarm by illuminating the major LED when the input relays are closed:

```
admin> new alarm relay
ALARM/relay read
admin> set enabled = yes
admin> set event = input-relay-closed
admin> set physical-address = { any-shelf any-slot 0 }
admin> set action alarm-led-major = on
admin> write
ALARM/relay written
```

The following commands create the `trap` profile for the specified events:

```
admin> new trap relay
TRAP/relay read
```

```
admin> community-name = public
admin> host-address = 135.17.134.31
admin> host-port = 2345
```

The following commands enable the test mode:

```
admin> inputrelaytest -p
Test input relay alarm is enabled
Remember to run "inputrelaytest -p" again to return to external input relay
alarm mode when finish the test!

LOG emergency, Shelf 1, Controller-1, Time: 10:35:05--
  Fri May 23 10:35:05 2003 - ALARM: Input Relay No. 1 OPEN

LOG emergency, Shelf 1, Controller-1, Time: 10:35:05--
  Fri May 23 10:35:05 2003 - ALARM: Input Relay No. 2 OPEN

LOG emergency, Shelf 1, Controller-1, Time: 10:35:05--
  Fri May 23 10:35:05 2003 - ALARM: Input Relay No. 3 OPEN

LOG emergency, Shelf 1, Controller-1, Time: 10:35:05--
  Fri May 23 10:35:05 2003 - ALARM: Input Relay No. 4 OPEN

LOG emergency, Shelf 1, Controller-1, Time: 10:35:05--
  Fri May 23 10:35:05 2003 - ALARM: Input Relay No. 5 OPEN

LOG emergency, Shelf 1, Controller-1, Time: 10:35:05--
  Fri May 23 10:35:05 2003 - ALARM: Input Relay No. 6 OPEN

LOG emergency, Shelf 1, Controller-1, Time: 10:35:05--
  Fry 23 10:35:05 2003 - ALARM: Input Relay No. 7 OPEN
```

The following commands close all relays:

```
admin> inputrelaytest -m
Set relay CLOSED mode
admin> inputrelaytest -O
All test input relay closed
LOG emergency, Shelf 1, Controller-1, Time: 10:45:36--
  Fri May 23 10:45:36 2003 - ALARM: Input Relay No. 1 CLOSED

LOG emergency, Shelf 1, Controller-1, Time: 10:45:36--
  Fri May 23 10:45:36 2003 - ALARM: Input Relay No. 2 CLOSED

LOG emergency, Shelf 1, Controller-1, Time: 10:45:36--
  Fri May 23 10:45:36 2003 - ALARM: Input Relay No. 3 CLOSED

LOG emergency, Shelf 1, Controller-1, Time: 10:45:36--
  Fri May 23 10:45:36 2003 - ALARM: Input Relay No. 4 CLOSED

LOG emergency, Shelf 1, Controller-1, Time: 10:45:36--
  Fri May 23 10:45:36 2003 - ALARM: Input Relay No. 5 CLOSED

LOG emergency, Shelf 1, Controller-1, Time: 10:45:36--
```

```
  Fri May 23 10:45:36 2003 - ALARM: Input Relay No. 6 CLOSED

LOG emergency, Shelf 1, Controller-1, Time: 10:45:36--
  Fri May 23 10:45:36 2003 - ALARM: Input Relay No. 7 CLOSED
```

The following commands simulates an individual input relay, relay 1, as open. The system response is shown below:

```
admin> inputrelaytest -m
Set relay OPEN mode
admin> inputrelaytest -1
Test input relay 1 open
admin>
LOG emergency, Shelf 1, Controller-1, Time: 10:46:47--
  Fri May 23 10:46:47 2003 - ALARM: Input Relay No. 1 OPEN
```

Displaying the status of input relays

The following sample command shows the status of the input relays:

```
admin> inputrelaytest -t
Test Input Relay Status
Item  Status
------------------------
 1    OPEN
 2    OPEN
 3    OPEN
 4    OPEN
 5    OPEN
 6    OPEN
 7    OPEN
```

The following sample commands shows the status of the external input relays:

```
admin> inputrelaytest -s
External Input Relay Status
Item  Status
------------------------
 1    OPEN
 2    OPEN
 3    OPEN
 4    OPEN
 5    OPEN
 6    OPEN
 7    OPEN
```

Configuring a bit-error rate test (BERT)

The bit-error rate test is an end-to-end test that evaluates the quality of a line. If enabled, an internal bits generator sends all-one bits for the duration specified to either a CPE or through an internal loop terminal node.

If the CPE and Stinger unit are connected and both are enabled for bit-error rate testing, the test runs between the two systems. If the test is enabled, the Stinger unit initiates the test by sending an embedded operations channel (EOC) message to the CPE to place its port into loopback mode. The CPE responds with an

acknowledgement. Once the test has completed, the CPE takes the port out of loopback mode and the port resumes normal operations.

If the Stinger unit and the CPE are not connected, the test runs within the 150-ohm DSL loop termination node on the port in the Stinger unit. If enabled, the port enters an analog loopback mode and undergoes bit-error rate testing. While undergoing the test, the port cannot pass data. Once the BERT has completed, the port is ready to train to a remote CPE.

Note In this software version, local and end-to-end BERTs work for the SHDSL/HDSL2 LIM operating in HDSL2 mode, but not for LIMs operating in SHDSL mode.

To run a BERT, set the `bert-enable` parameter in the `line-diag` profile for the line to `yes`. The test counts bit errors continuously for the interval specified by the `bert-timer` parameter.

Sample configuration

The following sample commands enable a BERT on port 1 in slot 4 for 5 minutes:

```
admin> read line-diag {1 4 1}
LINE-DIAG/{ shelf-1 slot-4 1 } read

admin> list
[in LINE-DIAG/{ shelf-1 slot-4 1 }]

admin> set bert-timer = 5

admin> set bert-enable = yes

admin> write
LINE-DIAG/{ shelf-1 slot-4 1 } written
```

The `line-diag-stat` profile includes parameters that report the status of the line and the result of the test. To determine the status of the BERT, use the `get` command to display the setting for the `bert-operation-state` parameter. For a list of all the possible states of the line, see the *Stinger Reference*. The BERT is complete if the value for the `bert-operation-state` parameter is `stopped`. For example:

```
admin> get line-diag-stat {1 4 1} bert-operation-state
[in LINE-DIAG-STAT/{ shelf-1 slot-4 1 }:bert-operation-state]
bert-operation-state = stopped
```

To show any BERT errors detected, display the setting for the `bert-error-counter` parameter. For example:

```
admin> get line-diag-stat {1 4 1} bert-error-counter
[in LINE-DIAG-STAT/{ shelf-1 slot-4 1 }:bert-error-counter]
bert-error-counter = 0
```

Testing DSL copper loops

The following features allow for testing of DSL copper loops. The galvanic isolation feature disconnects up to 48 ports on a Stinger line-interface module (LIM), leaving the lines open for testing. With the multiple port tone generation feature, you can send a trace tone to up to 48 ports simultaneously. The tone is obtained from an external generator connected to the external test terminal on a path selector module (PSM) or copper loop test (CLT) module.

You can use the `line-tests` profile or the `isolate` and `gen-tone` commands to perform these tests.

You can perform more comprehensive line tests by using the copper loop test (CLT) module. For more information, see the *Stinger Copper Loop Test (CLT) Module Guide*.

Using the `line-tests` profile

Each LIM has an associated `line-tests` profile. You use the `line-tests` profile to activate both the galvanic isolation and multiport tone tests. Following are the `line-tests` parameters with their default values:

```
[in LINE-TESTS]
physical-address* = { shelf-1 slot-5 0 }
clt-slot-number = slot-13
start-port = 0
end-port = 0
port-activation-array = [ no no no no no no no no no no no no no no +
port-status = [ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0+
specific-ports = no
test-type = gal-iso
test-terminal = external-tester-terminal
activate-test = no
```

Parameter	Heading
`physical-address`	Physical address of the LIM associated with this profile.
`clt-slot-number`	Slot number of the CLT module or PSM installed in the Stinger unit.
`start-port`	First port to be isolated during test. This parameter is valid only if `specific-ports` is set to `no`.
`end-port`	Last port to be isolated during test. All ports between `start-port` and `end-port` are isolated. This parameter is valid only if `specific-ports` is set to `no`.
`port-activation-array`	Ports that are isolated. A value of `yes` isolates the port or connects it to a tone generator. A value of `no` does not isolate or connect the port. This parameter is valid only if `specific-ports` is set to `yes`.
`port-status`	Status of each port on the LIM. A value equal to the slot number of the LIM indicates that the port is isolated or connected to a tone generator. A value of 0 indicates the port is not isolated or connected to a tone generator.
`specific-ports`	Whether port activation is controlled by the `port-activation-array` (`specific-ports` is set to `yes`).
`test-type`	Type of test. Specify `gal-iso` or `tone-gen`.

Parameter	Heading
test-terminal	CLT module or PSM terminal where the test tone is applied. Specify external-tester-terminal or aux-tester-terminal.
activate-test	Enable/disable a test. A value of yes disconnects any existing calls and begins the test. A value of no reconnects any disconnected calls and stops the test.

Galvanic isolation test

You activate a galvanic isolation test by configuring the line-tests profile or by using the the isolate command.

Using the line-tests profile

To isolate ports 3 through 5 of a LIM in slot 5, proceed as follows:

```
admin> read line-tests {1 5}
LINE-TESTS/{ shelf-1 slot-5 0 } read

admin> set start = 3

admin> set end = 5

admin> set activate = yes

admin> write
LINE-TESTS/{ shelf-1 slot-5 0 } written
```

As the lines are disconnected, you receive a series of error messages. For example:

```
LOG warning, Shelf 1, Slot 5, Time: 11:12:59--
[1/5/3/0] Network Problem, Cause code 001

LOG warning, Shelf 1, Slot 5, Time: 11:12:59--
[1/5/3/0] Network Problem, Cause code 002
```

If you list the line-tests profile again, the port-status parameter reports which ports are isolated. For example:

```
port-status = [ 0 0 5 5 5 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 +
```

Ports 3 through 5 remain disconnected until you set the activate-test parameter to no.

You can also select ports individually. To isolate only ports 3 and 9 on a LIM, proceed as follows:

```
admin> set port-activation 3 = yes

admin> set port-activation 9 = yes

admin> set specific-ports = yes

admin> set activate-test = yes

admin> write
```

To stop either test proceed as follows:

```
admin> set activate-test = no

admin> write
```

The system generates log messages as the tested lines are reconnected.

Using the `isolate` command

You use the `isolate` command to isolate either a range of ports or a list of individual ports. Its syntax is as follows:

- For a range of ports:

  isolate *shelf slot start-port - end-port*

- For individual ports:

  isolate *shelf slot p1 p2 .....*

- To deactivate the test:

  deisolate *shelf slot*

For example, to isolate ports 3 through 5 on a LIM in slot 5, proceed as follows:

```
admin> isolate 1 5 3 - 5
```

To isolate ports 3 and 9 only:

```
admin> isolate 1 5 3 9
```

To stop the test:

```
admin> deisolate 1 5
```

Multiport tone generation test

By connecting an external test tone generator to the external or auxiliary port on the CLT module or PSM, you can activate a multiport tone generation test by using the `line-tests` profile or `gen-tone` command.

Using the `line-tests` profile

The following sample commands apply a test tone to ports 3 through 5 of a LIM in slot 5 using a tone generator connected to the auxiliary terminals of the CLT module:

```
admin> set start = 3
admin> set end = 5
admin> set test-type = tone-gen
admim> set test-terminal = auxillary-tester-terminal
admin> set activate = yes
admin> write
LINE-TESTS/{ shelf-1 slot-5 0 } written
```

To perform the same test on ports 3 and 9, proceed as follows:

```
admin> set specific-ports = yes
admin> set port-activation 3 = yes
admin> set port-activation 9 = yes
admin> set test-type = tone-gen
admim> set test-terminal = auxillary-tester-terminal
admin> set activate = yes
```

```
admin> write
LINE-TESTS/{ shelf-1 slot-5 0 } written
```

To stop either test, proceed as follows:

```
admin> set activate-test = no
admin> write
```

Using the gen-tone command

You can use the **gen-tone** command to apply test tones on either a range of ports or a list of individual ports. Its syntax is as follows:

- For a range of ports:

  gen-tone *shelf slot* ext|aux *startport - endport*

- For individual ports:

  gen-tone *shelf slot* ext|aux *p1 p2 .....*

- To deactivate the test:

  degen-tone *shelf slot*

For example, to connect test tones to ports 3 through 5 on a LIM in slot 5 using the auxiliary port:

```
admin> gen-tone 1 5 aux 3 - 5
```

To connect test tones to ports 3 and 9 only using the external port, enter the following command:

```
admin> gen-tone 1 5 ext 3 9
```

To stop the test, enter the following command:

```
admin> degen-tone 1 5
```

Administering the SNMP Agent 9

To set up the Stinger unit as a Simple Network Management Protocol (SNMP) agent to work with SNMP managers, you must enable and configure the agent, establish its relationship and communications with remote managers, and manage SNMP interfaces from the TAOS command line, including establishing naming conventions for TAOS profiles configured via SNMP.

For information about SNMP management of Stinger ATM features, including the ATM Forum Private Network-to-Network Interface (PNNI) software, see the *Stinger SNMP Management of the ATM Stack Supplement*.

Overview of Stinger SNMP support

The Stinger unit supports Simple Network Management Protocol (SNMP), which is a standard way for computers to share networking information. An SNMP management system includes one or more *managers* and *agents* that communicate management information by means of SNMP.

Stinger unit as an SNMP agent

As an SNMP agent, a Stinger unit performs the network-management functions requested by an SNMP manager. An SNMP manager is a utility that runs on a network host. If an SNMP manager uses supported management information bases (MIBs), it can use `get` or `set` commands to query, administer, and configure the Stinger unit. When polled, the Stinger unit can send a message called a trap packet data unit (PDU) to inform the manager of network events. In addition, when certain

system events occur, the Stinger unit can use trap PDUs to send unsolicited information to the manager.

Requirement for a soft IP address

For an SNMP manager to access the Stinger SNMP agent, you must configure the Stinger unit with an IP address in the `ip-global` profile. For Stinger FS, Stinger FS+, Stinger LS, and Stinger RT units with redundant control modules, if you are using NavisAccess™ software, you must also configure a soft IP address for a backup connection. For information about configuring IP addresses, see the *Getting Started Guide* for your unit.

Overview of the `snmp` profile

The `snmp` profile contains the parameters that you use to activate and configure the Stinger SNMP agent. Following is a listing of the parameters in the `snmp` profile, shown with their default values:

```
admin> list
[in SNMP]
read-access-hosts = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0+
write-access-hosts = [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 +
engine-id = 80:00:02:11:03:00:c0:7b:4f:8a:56:00
engine-boots = 21
```

Table 9-1 lists parameters in the `snmp` profile and how you might use them to enable or configure SNMP features.

Table 9-1. SNMP parameters and associated tasks

Parameter	Task
`enabled`	Enabling/disabling the Stinger SNMP agent.
■ `read-community` ■ `read-write-enabled` ■ `read-write-community`	Enabling/disabling read-write access to the SNMP agent and set community strings. See "Enabling read-write access and setting community strings" on page 9-4 for additional information.
`enforce-address-security`	Enabling/disabling host address security. See "Configuring host address security" on page 9-4 for additional information.
■ `contact` ■ `location`	Identifying the contact information for and location of the SNMP device. See the *Stinger Reference* for additional information.
`queue-depth`	Specifying the maximum size of the queue for SNMP requests. Valid settings are from `0` through `1024`. The default setting `0` (zero) prevents the Stinger unit from dropping packets, no matter how far behind the SNMP subsystem gets. If a queue grows too large in a heavily loaded routing environment, the system can ultimately run out of memory.

Table 9-1. SNMP parameters and associated tasks (Continued)

Parameter	Task
csm-modem-diag	*Does not apply to the* Stinger *unit.*
snmp-message-type	Specifying the version of SNMP used by the Stinger SNMP agent. Specify one of the following values: ■ v1-and-v3 (the default)—The SNMP agent uses both SNMPv1 and SNMPv3 protocols. ■ v1-only—The SNMP agent uses only the SNMPv1 protocol and discards any other types of messages. ■ v3-only—The SNMP agent use only the SNMPv3 protocol and discards other types of messages. See "Configuring SNMPv3 USM privacy" on page 9-6 for additional information.
security-level	Specifying the level of security to use when generating messages. See "Configuring SNMPv3 USM privacy" on page 9-6 for additional information.
enable-vacm	Enabling/disabling the view-based access control model (VACM) on the Stinger unit. See "Configuring view-based access control" on page 9-13 for additional information.
notification-log-age-out	Specifying the number of minutes to keep a notification in a log before it is automatically removed. The default is 1440 minutes (24 hours). Specifying 0 (zero) keeps notifications in a log indefinitely. See the *Stinger Reference* for additional information.
bit-strings-allowed	Enabling/disabling the Stinger SNMP agent to report bits-type data in either bits format or numeric format. With the default setting of yes, the Stinger SNMP agent reports in bit string format. With the no setting, the Stinger SNMP agent reports in numeric format. See the *Stinger Reference* for additional information.
alarm-clear-table-limit	Specifying the maximum number of alarms that can be stored in alarmClearTable. See "Setting the maximum number of alarms in alarmClearTable" on page 9-18.

Activating the SNMP agent

You activate the SNMP agent by setting the enabled parameter in the snmp profile, as in the following example:

```
admin> read snmp
SNMP read

admin> set enabled = yes
```

```
admin> write
SNMP written
```

Securing the SNMP agent

TAOS provides the following means to secure the SNMP agent in the Stinger unit against unwanted access from remote SNMP managers, to specify the type of access granted to SNMP managers, and to configure encryption and authentication for the communications between the agent and managers:

- Ability to specify community strings when you enable read-write access.
- Enforcement of SNMP manager host authentication.
- Configuration of SNMPv3 messaging features such as authentication and encryption between the SNMP agent and manager. (This capability requires the network management software license.)
- Configuration of view-based access control model (VACM) features to control different types of access to various objects in the system. Control is applied on the basis of the security name in the request, the security level specified for the request, or the context name and object identifier (OID) of the object for which access is being attempted.

Enabling read-write access and setting community strings

Caution For security reasons, Lucent Technologies recommends that when you enable read-write access, you change the read-write community string from the well-known `write` value. By default, read-write access is disabled.

To set the community strings and enable read-write access, proceed as in the following example:

```
admin> set read-community = !3gtest0
admin> set read-write-enabled = yes
admin> set read-write-community = @456test!
admin> write
SNMP written
```

Configuring host address security

You can also enforce host address authentication before the agent accepts SNMP requests. Address security is optional but recommended. By enabling the `enforce-address-security` parameter in the SNMP profile, you exclude SNMP access from host SNMP manager addresses other than those you have specified. You create an `snmp-manager` profile to grant read and write access for an *unlimited* number of SNMP managers that use either SNMPv1 or SNMPv3.

Enabling host address security

To configure the unit to enforce host address security, proceed as follows:

```
admin> read snmp
SNMP read
admin> set enforce-address-security = yes
```

```
admin> write
SNMP written
```

Configuring the snmp-manager profile

You create an snmp-manager profile to identify the address of the host SNMP manger that sends SNMP requests to the SNMP agent and to define the type of access that is granted to the host.

Following is a listing of an unconfigured snmp-manager profile, shown with default settings:

```
[in SNMP-MANAGER/"" (new)]
name* = ""
active= no
write-access = no
snmp-message-type = v1-and-v3
```

Parameter	Setting
name	Name (up to 31 characters) or IP address (in dotted decimal notation) of the host SNMP manager that sends SNMP requests to the Stinger SNMP agent. If the Domain Name System (DNS) or Network Information Service (NIS) is supported, the system uses this name to look up the LAN address.
active	Enable/disable the processing of SNMP messages from a particular SNMP manager. Specify yes or no (the default).
write-access	Enable/disable write access for the SNMP manager. This parameter applies only if the active parameter is set to yes in the same snmp-manager profile. Specify one of the following settings: ■ yes—The SNMP manager has read and write access. ■ no (the default)—The SNMP manager has read-only access.
snmp-message-type	Whether the unit accepts SNMPv1 messages only, SNMPv3 messages only, or both SNMPv1 and SNMPv3 messages. This parameter applies only if the active parameter is set to yes in the same snmp-manager profile. Specify one of the following settings: ■ v1—Accept SNMPv1 messages only. ■ v3—Accept SNMPv3 messages only. ■ v1-and-v3 (the default)—Accept SNMPv1 and SNMPv3 messages. Stinger units support SNMPv3 user-based security model (USM) privacy and authentication. For more information, SNMPv3 USM authentication and privacy features, see "Configuring SNMPv3 USM privacy" on page 9-6.

Example of configuring host address security

The following example configures the Stinger unit to enforce host address security and grants a an SNMP manger called `remote1` read and write access to the unit by means of SNMPv3 only:

```
admin> read snmp
SNMP read
admin> set enforce-address-security = yes
admin> write
SNMP written
admin> new snmp-manager
SNMP-MANAGER/"" read
admin> set name = remote1
admin> set active = yes
admin> set write-access = yes
admin> set snmp-message-type = v3-only
admin> write
SNMP-MANAGER/remote1 written
```

Configuring SNMPv3 USM privacy

Stinger units support SNMPv3 user-based security model (USM) privacy and authentication. SNMPv3 USM is described in RFC 2574, *User-based Security Model for SNMPv3*.

Enabling privacy causes the Stinger unit to accept encrypted requests from an SNMP manager and send responses in encrypted format. The encryption uses a 64-bit Data Encryption Standard (DES) algorithm. The system uses your privacy password to generate a private key for the encryption.

To use SNMPv3 USM, you must have the network management software license installed on your Stinger unit.

Verifying the SNMPv3 license is enabled

The following command verifies that the network management license has been enabled on the system:

```
admin> get base network-management
[in BASE:network-management-enabled]
network-management-enabled = yes
```

If the network-management license is not enabled, the Stinger unit silently discards incoming queries if the SNMP message is version 3. For information about software licenses, contact your Lucent Technologies sales representative.

SNMPv3 USM features

SNMPv3 security management provides Stinger units with the following features:

- Authentication—Provides data integrity and data origin authentication. The message authentication is coded with either the message digest 5 (MD5) or the secure hash algorithm (SHA) function. See "Generating authentication keys" on page 9-9.

- Privacy—Protects messages from being copied and interpreted by unauthorized listeners on the network. "Generating privacy keys" on page 9-9.
- Timeliness—Protects against message delay or replay.
- Discovery—Allows an SNMP manager to obtain sufficient information about the Stinger units' SNMP agent to establish communication between an SNMP manager station and the Stinger units.
- GetBulkRequest—Added from SNMPv2 to allow the SNMPv3 manager to minimize the number of protocol exchanges required to retrieve a large amount of management information. The GetBulkRequest protocol data unit (PDU) allows an SNMPv3 manager to request as large a response as possible.

Enabling SNMPv3 USM privacy

The `security-level` parameter in the `snmp` profile specifies the security level of the SNMP agent when SNMPv3 is in use.

When configuring SNMPv3 USM privacy support, set the `security-level` parameter in the `snmp` profile to `auth-priv`, as the shown in the following example:

```
admin> read snmp
SNMP read

admin> set security-level = auth=priv

admin> write
```

With this setting, the system rejects all user transmissions with a security level of `none` or `auth-nopriv` by sending the error message `Unsupported Security Level`.

Using the `snmpv3-usm-user` profile

The `snmpv3-usm-user` profile contains the parameters that support SNMPv3 USM privacy. You create and edit user profiles in the `snmpv3-usm-user` profile. The following example lists the contents of the `snmp-usm-user` profile, shown with default settings:

```
[in SNMPV3-USM-USER/groupz]
name* =groupz
password = feow4873re
active-enabled = no
read-write-access = no
auth-protocol = md5-auth
priv-protocol = no-priv
```

```
auth-key =
priv-key =
```

Parameter	Setting
`name`	Username of an SNMP management station. Messages sent to or from the SNMP station on behalf of this name use the security parameters specified in this profile. Enter a string of up to 23 characters. You can include special characters by using the *\xNN* format with the ASCII code for the character. For example, the value `test\x20\x21` represents the following string: `test !`
`password`	A password, up to 20 characters in length, which maps to a 16-octet or 20-octet key in compliance with RFC 2574. Passwords are case sensitive and can include special characters if you use the *\xNN* format with the ASCII code for the character. For example, the value `test\x20\x21` represents the following string: `test !` This setting is required if `auth-protocol` is set to a value other than `no-auth`.
`active-enabled`	Enable/disable SNMPv3 user-based security model (USM) features for this user. The default value is `no`.
`read-write-access`	Enable/disable read-write access to the Stinger unit's MIBs for this user. With the default value `no`, the user has read access only, which enables viewing but not modification of the MIBs.
`auth-protocol`	Enable/disable authentication of messages sent on behalf of this user to or from the SNMP engine, and if enabled, the type of authentication protocol to be used. If this parameter is set to a value other than `no-auth`, the `password` parameter must specify the password to be used. Specify one of the following values: ■ `no-auth`—Disables authentication for this user. ■ `md5-auth` (the default value)—Enables authentication using the MD5 protocol. ■ `sha-auth`—Enables authentication using the SHA protocol.

Parameter	Setting
`priv-protocol`	Enable/disable encryption of messages sent on behalf of the user to or from the SNMP engine, and if enabled, the type of privacy protocol to be used. Specify one of the following values: ■ `no-priv` (the default)—No encryption is required and privacy is disabled. ■ `des-priv`—DES-based privacy is required. Incoming messages that are DES-encrypted are interpreted, and outgoing responses are encrypted using DES. Note that outgoing reports are not encrypted.
`auth-key`	Authentication key for SNMPv3 USM users. In most cases, you do not set this string directly. Instead, use the `snmpauthpass` command to generate the value. If you have permission to view passwords, the authentication key appears as a string with escape sequences for save and restore purposes. Otherwise, the authentication key appears as a row of asterisks. The default is null. For more information, see the *Stinger Reference*.
`priv-key`	Privacy key for SNMPv3 USM users. In most cases, you do not set this string directly. Instead, use the `snmpprivpass` command to generate the value. If you have permission to view passwords, the privacy key appears as a string with escape sequences for save and restore purposes. Otherwise, the privacy key appears as a row of asterisks. The default is null. For more information, see the *Stinger Reference*.

Generating authentication keys

You use the `snmpauthpass` command to automatically generate an authentication key for an SNMPv3 USM user. This command, which can be entered only from the primary control module, uses the following syntax:

`snmpauthpass` *`username password`*

Replace *username* with the SNMPv3 USM user for whom an authentication key is being generated, and *username* with the password used for generating the authentication key.

Note The password you specify is not stored in the system. It is used to generate an authentication key when the user is authenticated. The key is stored in the system.

To generate an authentication key of the user `robin` with the password `abc123`, proceed as follows:

```
admin> snmpauthpass robin abc123
```

Generating privacy keys

The `snmpprivpass` command can be used to automatically generate a privacy key for an SNMPv3 USM user. The command uses the following syntax:

snmpprivpass *username password*

Replace *username* with the SNMPv3 USM user for whom a privacy key is being generated, and *password* with the password used for generating the privacy key.

Note The password you specify is not stored in the system. It is used to generate a privacy key when the user is authenticated. The key is stored in the system.

To generate the privacy key of the user `robin` with the password `abc123, proceed as follows`:

```
admin> snmpprivpass robin abc123
```

Example of SNMPv3 USM configuration

To configure the USM features for a user, specify a name for the profile and set the `active-enabled` parameter to `yes`. You must also specify a password if the `auth-protocol` parameter is set to anything but `no-auth`.

The following commands specify the use of MD5 authentication for messages sent on behalf of a user named `testv3` to or from the SNMP engine. The user is assigned read-write access to the Stinger unit's MIBs.

```
admin> new snmpv3-usm-user testv3
SNMPV3-USM-USER/testv3 read
admin> set active-enabled = yes
admin> set read-write-access = yes
admin> set priv-protocol = des-priv
admin> write
SNMPV3-USM-USER/testv3 written
admin> snmpauthpass testv3 abc123
admin> snmpprivpass testv3 abc123
admin> read snmpv3-usm-user testv3
SNMPV3-USM-USER/testv3 read
admin> list
[in SNMPV3-USM-USER/testv3]
name* = testv3
active-enabled = yes
read-write-access = yes
auth-protocol = md5-auth
priv-protocol = des-priv
auth-key = \xfd\xcd\xb2V\xa7\x81\xa7\x89n"\xd5\x02\x8b\xb2\xe7K
priv-key = \xfd\xcd\xb2V\xa7\x81\xa7\x89n"\xd5\x02\x8b\xb2\xe7K
```

Restricting the agent to SNMPv3

The following commands cause the SNMP agent to use only SNMPv3 and to check a user's security level before allowing access:

```
admin> read snmp
SNMP read
admin> set snmp-message-type = v3-only
admin> set security-level = auth-nopriv
```

```
admin> write
SNMP written
```

SNMPv3 notifications

The Stinger unit authenticates and encrypts protocol data units (PDUs) as required by SNMPv3, and generates traps in SNMP version 2 (SNMPv2) Trap2 format. Depending on your configuration, a Stinger unit can send PDUs in SNMPv2 format or formats supported by TAOS 9.0-126 and earlier releases. You can specify the destinations for traps and the format of outgoing trap PDUs. The corresponding MIBs are `snmp-target-mib` and `snmp-notification-mib`.

SNMPv3 notifications support enables you to configure the Stinger unit to perform the following tasks:

- Send SNMPv1 traps (trap PDUs) or SNMPv2 traps (Trap2 PDUs).
- Send traps to a specified IP address and port.
- Send Trap2 PDUs with different levels of security.
- Send Trap2 PDUs with different usernames.

The SNMPv3 notifications feature follows the specifications in RFC 2573.

Configuring SNMPv3 notifications support

To set up SNMPv3 notifications supports from the command-line interface, perform the following steps:

1 Create an `snmpv3-notification` profile, and set a tag to the profile. (See "Configuring an snmpv3-notification profile" on page 9-12.)

2 Create an `snmpv3-target-param` profile. (See "Configuring an snmpv3-target-param profile" on page 9-12.)

   – Set the message-processing model to the `v1` or `v3` option

   – Set the security model to the `v1` or `v3-usm` option. If the `v3-usm` option is selected, set the `security-name` parameter to a valid `snmpv3-usm-user` profile name.

3 Create a `trap` profile. For additional information about creating a trap profile, see "Configuring the trap profile" on page 9-20.

   – Set the name, destination IP address, and destination port

   – Add tag values to the `notify-tag-list` parameter. This tag list must contain tags that were set in the `snmpv3-notification` profile. You can configure multiple tags in this tag list, separated by spaces.

   – Set `target-params-name` to the name of the `snmpv3-target-param` profile. All the notification profiles in the system will find `trap` profiles with matching tags. The parameters in the `trap` profiles are used to send traps to the network.

Note When you upgrade to software that supports the SNMPv3 notifications feature, the system automatically creates an `snmpv3-notification` profile and an `snmpv3-target-param` profile; both are called `default`. Therefore, SNMPv1 traps configured in an earlier version of the software are still generated when you upgrade. You need not create new profiles. However, removing or modifying the `default` profiles might affect the transmission of SNMPv1 traps.

Configuring an snmpv3-notification profile

Following are the snmpv3-notification parameters and their default settings:

```
[in SNMPV3-NOTIFICATION/"" (new)]
name* = ""
active-enabled = no
tag = ""
type =
```

Parameter	Setting
name	Unique name for the profile, up to 16 characters.
active-enabled	Enable/disable generation of notifications. Specify yes to use this profile to generate notifications. The default value, no, specifies that the profile is not used to generate notifications.
tag	Value linking the snmpv3-notification profile with the trap profile that specifies the host address to which notification messages are sent. Specify up to 255 characters. The default is null.
type	*Not currently implemented.*

Configuring an snmpv3-target-param profile

Following are the snmpv3-target-param profile parameters and their default settings:

```
[in SNMPV3-TARGET-PARAM/""]
name* = ""
active-enabled = no
msg-proc-model = v1
security-model = v1
security-name =
security-level = none
```

Parameter	Setting
name	Unique name for the profile, up to 16 characters. The default is null.
active-enabled	Enable/disable generation of notifications. Specify yes to use this profile for generating notifications. The default value, no, specifies that the profile is not used to generate notifications.
msg-proc-model	Message-processing model to use when generating SNMP messages. The default setting, v1, specifies SNMP version 1. Specify v3 for SNMPv3 notifications support.

Parameter	Setting
security-model	Security model to use when generating SNMP messages. Specify one of the following values: ■ v1 (the default)—SNMPv1 security model. This setting is valid only if msg-proc-model is set to v1. ■ v3-usm—SNMPv3 USM. For SNMPv3 notifications support, specify v3-usm. This setting is valid only if msg-proc-model is set to v3. For the snmpv3-target-param profile to have any effect when security-model is set to v3-usm, the name parameter in the snmpv3-usm-user profile must match the security-name parameter in the snmpv3-target-param subprofile.
security-name	Security name of up to 22 characters that identifies the user on whose behalf SNMPv3 USM messages are generated. The default is null. For the security-name parameter to apply, set security-model to v3-usm.
security-level	Level of security to use when generating messages. Specify one of the following values: ■ none (the default)—No authentication and no privacy. ■ auth-nopriv—Authentication and no privacy. ■ auth-priv—Authentication and privacy. For the auth-priv to apply, you must set the priv-protocol and priv-password parameters in the snmpv3-usm-user profile.

Configuring view-based access control

As described in RFC 2575, the view-based access control model (VACM) defines a mechanism for SNMP entities to determine whether a specific type of access (read, write, or notify) to a particular object is allowed. RFC 2575 defines a structured configuration that can check accessibility for each get or set request received and notify request sent.

With VACM enabled, you can configure the system to control different types of access to various objects in the system on the basis of the security name in the request, the security level specified for the request, or the context name and object identifier (OID) of the object for which access is being attempted. You can select read (get), write (set), and notify (trap or trap2) access.

You configure VACM at the command-line interface by performing the following tasks:

1 Enable VACM by setting the enable-vacm parameter to yes in the snmp profile.

2 Map a security name and security model in an incoming or outgoing message to a security group by setting the parameters in the vacm-security-group profile.

3 Specify view names for different kinds of access (read, write, notify) by setting parameters in the vacm-access profile. A view specifies whether a given OID is accessible.

4 Define views by setting parameters in the vacm-view-tree profile.

Enabling VACM

To enable VACM, set the `enable-vacm` parameter to `yes` in the `snmp` profile. With this setting, each object in each incoming request (GET/SET/GETNEXT/GETBULK) and each object in the sysTrapOID of each outgoing trap (TRAP2) is verified for VACM access.

The default value of `no` disables VACM, allowing access to all objects in the system. However, the unit still uses security based on SNMPv1 community strings and SNMPv3 USM (if enabled) to determine access.

Mapping a security name and security model to a security group

To map a security name and security model to a security group, set the parameters in the `vacm-security-group` profile. Following is a listing of the profile's default values:

```
[in VACM-SECURITY-GROUP/{ v1 "" } (new)]
security-properties* = { v1 "" }
active = no
group-name = ""

[in VACM-SECURITY-GROUP/{ v1 "" }:security-properties (new) (changed)]
security-model = v1
security-name = ""
```

Parameter	Setting
`active`	Enable/disable VACM. Specify `yes` to enable VACM or `no` (the default) to disable it.
`group-name`	Group name. The default is null.
`security-properties: security-model`	Security model in use for an incoming or outgoing message: ■ `v1` (the default)—The SNMPv1 security model. ■ `v3-usm`—SNMPv3 USM. For VACM support, specify `v3-usm`.
`security-properties: security-name`	USM username associated with an incoming or outgoing message. The default is null.

For example, the following commands configure SNMPv3 USM for a USM user called `joe` and a group called `groupNY`:

```
admin> new vacm-security-group
VACM-SECURITY-GROUP/{ v1 "" } read

admin> list
[in VACM-SECURITY-GROUP/{ v1 "" } (new)]
security-properties* = { v1 "" }
active = no
group-name = ""

admin> set active = yes

admin> set group-name = groupNY

admin> list security-properties
[in VACM-SECURITY-GROUP/{ v1 "" }:security-properties (new) (changed)]
```

```
security-model = v1
security-name = ""
admin> set security-model = v3-usm
admin> set security-name = joe
(New index value; will save as new profile VACM-SECURITY-GROUP/{ v3-usm joe
}.)
admin> write
VACM-SECURITY-GROUP/{ v3-usm joe } written
```

Specifying view names for different types of access

To map a group name, context prefix, context name, security model, and security level to a view name, set parameters in the `vacm-access` profile. Following is a listing of the profile's default values:

```
[in VACM-ACCESS/{"" "" v1 none }]
access-properties* = { {"" "" v1 none } }
active = no
match-method = exact-match
read-view-name = ""
write-view-name = ""
notify-view-name = FullView
admin> list access-properties
group-name = ""
context-prefix = ""
security-model = v1
security-level = none
```

Parameter	Setting
`active`	Enable/disable the view. Specify `yes` to enable the view or `no` (the default) to disable it.
`group-name`	Group name. The default is null.
`match-method`	Context-match method. `exact-match` (the default) specifies that the entire context name must be matched. `prefix-match` specifies that only the prefix specified by `context-prefix` must be matched.
`read-view-name`	Name of the view for read access. The default is null.
`write-view-name`	Name of the view for write access. The default is null.
`notify-view-name`	Name of the view for notify access. The default is null.
`access-properties: context-prefix`	Prefix for a given context. The default is null. The setting for the `match-method` parameter determines whether the context name is matched exactly or the prefix alone is matched.
`access-properties: security-model`	Security model in use. ■ `v1` (the default)—The SNMPv1 security model. ■ `v3-usm`—SNMPv3 USM. For VACM support, specify `v3-usm`.

Parameter	Setting
access-properties: security-level	Security level: ■ none (the default)—No authentication and no privacy. ■ auth-priv—Authentication and privacy. ■ auth-nopriv—Authentication and no privacy.

For example, to specify a view for read access for a group called groupSF with SNMPv3 USM authentication, and privacy enabled, enter the following commands:

```
admin> new vacm-access
VACM-ACCESS/{ "" "" v1 no+ } read

admin> list
[in VACM-ACCESS/{ "" "" v1 no+ } (new)]
access-properties* = { "" "" v1 no+ }
active = no
match-method = exact-match
read-view-name = ""
write-view-name = ""
notify-view-name = ""

admin> set active = yes

admin> set read-view-name = view1

admin> list access-properties
[in VACM-ACCESS/{ "" "" v1 no+ }:access-properties (new) (changed)]
group-name = ""
context-prefix = ""
security-model = v1
security-level = none

admin> set group-name = groupSF

admin> set security-model = v3-usm

admin> set security-level = auth-priv

admin> write
VACM-ACCESS/{ groupSF "" v3-usm auth-priv } written Defining views
```

Defining views

To define a view, set parameters in the vacm-view-tree profile. Following is a listing of the profile's default values:

```
[in VACM-VIEW-TREE/{ "" "" }]
tree-properties* = { "" "" }
active = no
tree-mask = ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff
tree-type = included

view-name = ""
view-tree-oid = ""
```

To define a view, set the following parameters:

Parameter	Setting
active	Enable/disable the view. Specify yes to enable the view or no (the default) to disable it.
tree-mask	Mask (in hexadecimal format) for comparing subidentifiers in the OID. To disable the comparing of a subidentifier, set the corresponding mask bit to 0 (zero).
tree-type	Whether the OID is accessible. For the OID to be accessible, specify included (the default). If you specify excluded, the OID is not accessible.
tree-properties: view-name	Name of the view. The default is null. The system determines whether the view contains a given OID by comparing it with view-tree-oid.
tree-properties: view-tree-oid	OID in dotted decimal format. The default is null.

For example, to define a view called view1 with an OID of 1.3.6.1.4.1.529, enter the following commands:

```
admin> new vacm-view-tree
VACM-VIEW-TREE/{ "" "" } read

admin> list
[in VACM-VIEW-TREE/{ "" "" } (new)]
tree-properties* = { "" "" }
active = no
tree-oid-mask = ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff
tree-type = included

admin> set active = yes

admin> list tree-properties
[in VACM-VIEW-TREE/{ "" "" }:tree-properties (new) (changed)]
view-name = ""
view-tree-oid = ""

admin> set view-name = view1

admin> set view-tree-oid = 1.3.6.1.4.1.529
(New index value; will save as new profile VACM-VIEW-TREE/{ view1
1.3.6.1.4.1.529 }.)

admin> write
VACM-VIEW-TREE/{ view1 1.3.6.1.4.1.529 } written
```

Configuring alarm settings for the alarm MIB

Stinger units support alarm MIBs as described in draft-ietf-disman-alarm-mib-04.txt. The MIBs provide the following information:

- All possible alarms in the system
- Currently active alarms in the system

- Cleared alarms in the system

Setting the maximum number of alarms in alarmClearTable

To set the maximum number of alarms in alarmClearTable, set the alarm-clear-table-limit parameter in the snmp profile. Specify a value from 1 through 200. The default value is 100. The following sample commands specify that up to 150 alarms can be stored in alarmClear Table:

```
admin> read snmp
SNMP read
admin> set alarm-clear-table-limit = 150
admin> write
SNMP written
```

Clearing alarms from alarmActiveTable and alarmClearedTable

To clear the alarms in alarmActiveTable and alarmClearTable of the alarm MIB, disable the associated trap profile by setting the active-enabled parameter in the trap profile to no. If the trap profile is disabled, the alarm model table reports RowStatus as NOT_IN_SERVICE.

Deleting an alarm model table

To delete an alarm model table, delete the corresponding trap profile.

Configuring SNMP traps

Stinger units generate traps (notifications) for important events. When a trap is generated by a certain event, the system sends a trap protocol data unit (PDU) to a specified host. You create and enable traps and specify their destination using a trap profile. You cannot configure traps by way of SNMP.

For information about profile and parameters that support threshold traps in the ADSL MIB, see "Configuring alarms for ADSL threshold values" on page 3-10.

For information about configuring SNMPv3 traps, see "SNMPv3 notifications" on page 9-11.

Creating a trap profile

You create a trap profile and assign it a name using the new command. A typical name might be the name of the destination host to which you are sending the trap PDUs. You can specify a name of up to 31 characters.

```
admin> new trap remote1
TRAP/remote1 read
```

As shown in the following example, when you list the profile, the name that you specify when you create the trap profile becomes the value of the host-name parameter. The rest of the parameters are shown with their default settings.

```
[in TRAP/remote1 ]
host-name* = remote1
active-enabled = yes
community-name = ""
host-address = 0.0.0.0
```

```
host-port = 162
inform-time-out = 1500
inform-retry-count = 4
notify-tag-list = default
target-params-name = default
notification-log-enable = no
notification-log-limit = 50
alarm-enabled = yes
security-enabled = no
port-enabled = no
slot-enabled = no
coldstart-enabled = yes
warmstart-enabled = yes
linkdown-enabled = yes
linkup-enabled = yes
ascend-enabled = yes
console-enabled = yes
use-exceeded-enabled = yes
password-enabled = yes
fr-linkup-enabled = yes
fr-linkdown-enabled = yes
event-overwrite-enabled = yes
radius-change-enabled = yes
mcast-monitor-enabled = yes
lan-modem-enabled = yes
slot-profile-change-enabled = yes
power-supply-enabled = yes
authentication-enabled = yes
config-change-enabled = yes
sys-clock-drift-enabled = yes
suspect-access-resource-enabled = yes
ospf-enabled = no
ospf-if-config-error-enabled = no
ospf-if-auth-failure-enabled = no
ospf-if-state-change-enabled = no
ospf-if-rx-bad-packet = no
ospf-tx-retransmit-enabled = no
ospf-nbr-state-change-enabled = no
ospf-virt-if-state-change-enabled = no
ospf-virt-if-rx-bad-packet = no
ospf-virt-if-tx-retransmit-enabled = no
ospf-virt-nbr-state-change-enabled = no
ospf-originateLsa-enabled = no
ospf-maxAgeLsa-enabled = no
ospf-lsdb-overflow-enabled = no
ospf-approaching-overflow-enabled = no
watchdog-warning-enabled = yes
controller-switchover-enabled = no
call-log-serv-change-enabled = yes
wan-line-state-change-enabled = yes
call-log-dropped-pkt-enabled = yes
lim-sparing-enabled = no
```

```
interface-sparing-enabled = no
secondary-controller-state-change-enabled = no
pctfi-trunk-status-change-enabled = yes
no-resource-available-enabled = yes
dsl-thresh-trap-enabled = no
atm-pvc-failure-trap-enabled = no
atm-ima-alarm-trap-enabled = no
ascend-link-down-trap-enabled = no
ascend-link-up-trap-enabled = no
snmp-illegal-access-attempt = no
hdsl2-shdsl-threshold-traps-enabled = yes
clock-change-trap-enabled = no
oam-timeout-trap-enabled = no
ascend-adsl-trap-enabled = no
ascend-multicast-link-trap-enabled = no
ascend-cac-fail-trap-enabled = no
ascend-cac-fail-trap-enabled = no
spvc-target-cac-fail-trap-enabled = yes
heart-beat-trap-enabled = no
ascend-flash-card-trap-enabled = yes
ascend-sw-mismatch-trap-enabled = no
ascend-hashcode-mismatch-trap-enabled = no
```

"Trap classes" on page 9-21 describes the trap parameters contained in the `trap` profile. For additional information about these parameters, see the *Stinger Reference*.

Configuring the `trap` profile

You must also activate a trap and specify a destination host and host port. The following parameters in the `trap` profile configure these settings:

Parameter	Setting
`active-enabled`	Enable/disable the system to send traps to the host specified by this profile: ■ `yes`—The system sends traps defined by this profile. ■ `no`—Traps specified by this profile are not sent.
`host-address`	IP address to which traps are sent. The default setting is `0.0.0.0`. If the host address is zero and a name service such as DNS or Network Information Service (NIS) is supported, you can specify the hostname instead. The system uses the name to look up the host address.
`host-port`	Port to which traps are sent. Specify a number from `1` to `65535`. The default setting is `162`.

The following sample commands instruct the unit to send traps to an SNMP manager at the IP address 1.1.1.1:

```
admin> read trap remote1
TRAP remote1 read
```

```
admin> set host-address = 1.1.1.1
admin> write
TRAP remote1 written
```

Trap classes

Traps are grouped into classes: alarm events, security events, port or slot state change, and OSPF events. These classes allow for enabling or disabling sets of traps. When a trap class is enabled, you can enable or disable individual traps within that class. Table 9-1 through Table 9-5 list the individual traps that belong to each trap class.

The following parameters in the `trap` profile represent the trap classes, shown with their default settings:

```
[in TRAP/""]
alarm-enabled = yes
security-enabled = no
port-enabled = no
slot-enabled = no
ospf-enabled
```

Parameter	Setting
`alarm-enabled`	Enable/disable an alarm class events. For details, see "Alarm class traps" on page 9-21.
`security-enabled`	Enable/disable security class events. For details, see "Security class traps" on page 9-24.
`port-enabled`	Enable/disable port class events. For details, see "Port class trap" on page 9-25.
`slot-enabled`	Enable/disable slot class events. For details, see "Slot class trap" on page 9-26.
`ospf-enabled`	Enable/disable OSPF class events. For details, see "OSPF class traps" on page 9-26.

Note Enabling an individual trap has no effect if the trap class to which it belongs is disabled.

Alarm class traps

By default, the alarm class is enabled. Table 9-2 lists the events in the alarm class and the parameters you use to enable or disable each individual trap.

For a Stinger unit to send a trap for the events listed in Table 9-2, accept the default setting of `yes` for the `alarm-enabled` parameter and enable the parameter for that specific event.

If the `alarm-enabled` parameter is set to `no`, the unit does not send traps for any of the events listed in Table 9-2.

Table 9-2. Parameters that enable or disable traps in the alarm class

Event	Parameter	Trap
Unit reinitialized itself in such a way that the configuration of the SNMP manager or of the system itself might be altered.	`coldstart-enabled`	`ColdStart`
Unit reinitialized itself so that neither the configuration of the SNMP manager nor that of the system itself was altered.	`warmstart-enabled`	`WarmStart`
Failure in a communication link between the unit and the SNMP manager.	`linkdown-enabled`	`LinkDown`
Communication link between the unit and the SNMP manager came back up.	`linkup-enabled`	`LinkUp`
A data link connection identifier (DCLI) was reinitialized.	`fr-linkup-enabled`	`FRLinkUp`
A DLCI has become inactive.	`fr-linkdown-enabled`	`FRLinkDown`
New event has overwritten an unread event. Once the trap has been sent, additional overwrites do not cause another trap to be sent until at least one table's worth of new events have occurred.	`event-overwrite-enabled`	`EventOverwrite`
Digital modem has been moved to the suspect list.	`lan-modem-enabled`	`LanModem`
Change in the state of a power-supply module. The module might have been added or removed.	`power-supply-enabled`	`powerSupplyStateChange` `powerSupplyOperationalStateChange`
System configuration was modified or a new software version was loaded.	`config-change-enabled`	`ConfigChange`
System clock drifted but could not be corrected.	`sys-clock-drift-enabled`	`SysClockDrifted`
T1000 module has received four or more calls for which it cannot establish a connection. The module is not assigned to terminate calls until all available resources are exhausted.	`suspect-access-resource-enabled`	`SuspectAccessResrc`
Watchdog warning has occurred. See "Configuring SNMP watchdogs" on page 9-35.	`watchdog-warning-enabled`	`WatchdogWarning`

Table 9-2. Parameters that enable or disable traps in the alarm class (Continued)

Event	Parameter	Trap
Change in primary control module in a unit with redundant control modules.	`controller-switchover-enabled`	`Controllerswitchover`
Change in the state of an E1 or T1 line.	`wan-line-state-change-enabled`	`WanLineStateChange`
The value of the `callLoggingDroppedPacketCount` variable changed from 0 to 1 (which indicates that packets are being dropped) or from 1 to 0 (which indicates that packets are no longer being dropped) in the call-logging MIB.	`call-log-dropped-pkt-enabled`	`CallLogDroppedPkt`
LIM redundancy has taken effect.	`lim-sparing-enabled`	`sparingSlotStatusChange`
LIM port redundancy has taken effect.	`interface-sparing-enabled`	`interfaceSparing`
Change in state of the secondary control module.	`secondary-controller-state-change-enabled`	`CntrReduAvail`
No resources are available to answer a call.	`no-resource-available-enabled`	`NoResourceAvailable`
Digital subscriber line (DSL) threshold has been reached. See "Configuring alarms for ADSL threshold values" on page 3-10.	`dsl-thresh-trap-enabled`	`dslThreshTrap`
Failure occurred on a PVC or soft PVC.	`atm-pvc-failure-trap-enabled`	`atmPvcFailureEnabled`
Failure occurred on with an IMA logical port.	`atm-ima-alarm-trap-enabled`	`atmimaalarmtrapenabled`
A module has been reset.	N/A. The system always sends traps when the corresponding event occurs and the alarm class is enabled. You cannot disable these traps individually.	`slotCardReset`
Reason for the last system reset.		`sysLastRestartReason`
ADSL link failed to initialize.		`AdslInitFailureTrap`
Failure in the a communication link between the Stinger SNMP agent and SNMP manager.	`ascend-link-down-trap-enabled`	`ascendLinkDown`

Table 9-2. Parameters that enable or disable traps in the alarm class (Continued)

Event	Parameter	Trap
Reestablishment of a failed communication link between the Stinger SNMP agent and SNMP manager.	ascend-link-up-trap-enabled	ascendLinkUp
A multicast group join activity has occurred.	ascend-multicast-link-trap-enabled	multicastLinkUpTrap
A multicast group leave activity has occurred.	ascend-multicast-link-trap-enabled	multicastLinkDownTrap
Connection admission control (CAC) failure for an ATM connection has occurred.	ascend-cac-fail-trap-enabled	cacfail
Soft permanent virtual circuit (SPVC) target call failure has occurred.	spvc-target-cac-fail-trap-enabled	To be provided.
Operations, administration, and maintenance (OAM) loopback and continuity test has timed out.	oam-timeout-trap-enabled	oamtimeoutTrap
OAM segment reports an AIS, LOC, or RDI defect.	oam-timeout-trap-enabled	atmOamDefectSegTrap
OAM end-to-end flow reports an AIS, LOC, or RDI defect.	oam-timeout-trap-enabled	atmOamDefectE2eTrap
The primary and secondary control modules have different TAOS versions.	ascend-sw-mismatch-trap-enabled	slotSWMatchingTrap
The primary and secondary control modules have different software licenses enabled.	ascend-hashcode-mismatch-trap-enabled	cntrHashcodeMatchingTrap

Security class traps

By default, the security class is disabled. To enable the Stinger unit to send one or more of the traps listed in Table 9-3, set the `security-enabled` parameter to `yes`:

```
[in TRAP/""]
admin> security-enabled = yes

admin> write
TRAP/test written
```

Table 9-3. Parameters that enable or disable traps in the security class

Event	Parameter	Trap
Authentication failure occurred.	`authentication-enabled`	`authentication`
Console has changed state. The console entry can be read to determine its current state.	`console-enabled`	`console`
Specific port has exceeded the number of DS0 minutes allocated to it.	`use-exceeded-enabled`	`useexceeded`
Maximum number of login attempts for a Telnet session has been exceeded.	`password-enabled`	`password`
New RADIUS server has been accessed. This trap returns the objectID and IP address of the new server.	`radius-change-enabled`	`radiuschange`
Call-logging server change has occurred.	`call-log-serv-change-enabled`	`calllogservchange`
SNMP access is disabled for the entire system, or the host in question was not authorized to access and/or to perform a `set` operation to the system. Only up to 10 Illegal Access traps and 10 Authentication Failure traps are generated over a 10-minute period. If the number of these traps exceeds this limit, the remaining traps are dropped.	`snmp-illegal-access-attempt`	`snmpIllegalAccessAttempt`

Port class trap

By default, the port class is disabled. For the Stinger unit to send the trap listed in Table 9-4, you must set the `port-enabled` parameter to `yes`.

```
[in TRAP/""]
port-enabled = yes
```

If the `port-enabled` parameter is set to `no`, the unit does not send the trap listed in Table 9-4.

Table 9-4. Parameter that enables or disables traps in the port-state class

Event	Parameter	Traps in port class
Change in the state of a host interface. All port connections are monitored in a state machine and reported by means of this trap.	`ascend-enabled`	`Ascend`

Slot class trap

By default, the slot class is disabled. For the Stinger unit to send the trap listed in Table 9-5, the following parameter must be set to `yes`:

```
[in TRAP/""]
slot-enabled = yes
```

If the `slot-enabled` parameter is set to `no`, the unit does not send the trap listed in Table 9-5.

Table 9-5. Parameter that enables or disables traps in the slot class

Event	Parameter	Trap
Change of state in a host interface. All port connections are monitored in a state machine and reported by means of this trap.	`slot-profile-change-enabled`	`SlotProfileChange`
Change in clock source.	`clock-change-trap-enabled`	`Clockchange`

OSPF class traps

Stinger units support OSPF class traps as defined in RFC 1850, *OSPF Version 2 Management Information Base*. By default, OSPF traps are disabled. To generate an OSPF trap when an event shown in Table 9-6 occurs, enable OSPF traps either in the `trap` profile or by setting the corresponding bit in the MIB object, `ospfSetTrap`, defined in RFC 1850. You must also enable the individual trap that represents the trap condition.

To enable OSPF traps in the `trap` profile, set `ospf-enabled` to `yes`. If `ospf-enabled` is set to `no` (the default), the unit does not send traps for any of the events listed in Table 9-6.

Table 9-6. Parameters that enable or disable traps in the OSPF class

Event	Parameter	Trap
Configuration error types 1 through 9, as defined in RFC 1850. Possible failure to form an adjacency. Traps for error type 10 (`optionMismatch`) are not currently supported.	`ospf-if-config-error-enabled`	`OSPF Trap 4`
Packet received on a nonvirtual interface from a router whose authentication key or type conflicts with the Stinger unit's authentication key or type.	`ospf-if-auth-failure-enabled`	`OSPF Trap 6`
Change in the state of a nonvirtual OSPF interface when the interface state regresses or progresses to a terminal state. For example, the state of the OSPF interface on a Stinger unit can regress from DR (designated router) to Down (unusable), or can progress to a terminal state of point-to-point (operational for point-to-point or virtual connections), DR Other (linked to a designated router on another network), or Backup (BDR). For details about interface state changes, see RFC 2328.	`ospf-if-state-change-enabled`	`OSPF Trap 16`
OSPF packet has been received on a nonvirtual interface that cannot be parsed	`ospf-if-rx-bad-packet`	`OSPF Trap 8`
OSPF packet has been retransmitted on a nonvirtual interface. All packets that are retransmitted are associated with a link-state database (LSDB) entry. The link-state type, link-state ID, and router ID identify the link-state database entry.	`ospf-tx-retransmit-enabled`	`OSPF Trap 10`

Table 9-6. Parameters that enable or disable traps in the OSPF class (Continued)

Event	Parameter	Trap
Change in the state of a nonvirtual OSPF neighbor. This trap is generated when the neighbor state regresses. For example, a neighbor's state can regress from Attempt (this neighbor needs Hello packets) or Full (this neighbor is fully adjacent) to 1-Way (communication with this neighbor is unidirectional) or Down (no recent information was received from this neighbor). Or it can progress to a terminal state like 2-Way (communication is bidirectional) or Full. A designated router transitioning to Down also causes the system to generate this trap or when a neighbor transitions from or to Full on NBMA and broadcast networks. For details about state changes, see RFC 2328.	`ospf-nbr-state-change-enabled`	`OSPF Trap 2`
Change in the state of a virtual OSPF interface when the interface state regresses (for example, from point-to-point to down) or progresses to a terminal state, such as point-to-point.	`ospf-virt-if-state-change-enabled`	`OSPF Trap 1`
A Stinger unit virtual interface received an OSPF packet that cannot be parsed.	`ospf-virt-if-rx-bad-packet`	`OSPF Trap 9`
An OSPF packet has been retransmitted on a virtual interface. All packets that are retransmitted are associated with a link-state database entry. The link-state type, link-state ID, and router ID are used to identify the link-state database entry.	`ospf-virt-if-tx-retransmit-enabled`	`OSPF Trap 11`
Change in state of an OSPF virtual neighbor.	`ospf-virt-nbr-state-change-enabled`	`OSPF Trap 3`
A new LSA has been originated by this router due to a topology change.	`ospf-originatelsa-enabled`	`OSPF Trap 12`
An LSA in the Stinger unit's link-state database has reached its maximum age.	`ospf-maxagelsa-enabled`	`OSPF Trap 13`
The number of LSAs in the Stinger unit's link-state database has exceeded the maximum limit.	`ospf-lsdb-overflow-enabled`	`OSPF Trap 14`
The number of LSAs in the Stinger unit's link-state database has exceeded 90 percent of the `OSPFExtLsdbLimit`.	`ospf-approaching-overflow-enabled`	`OSPF Trap 15`

Example of setting an OSPF trap

The following commands cause the system to generate traps when the Stinger unit receives a packet from an OSPF router in which a configuration mismatch (such as an invalid OSPF version number or an address conflict) or an authentication failure occurs:

```
admin> read trap monitor-ospf
TRAP/monitor-ospf read
admin> set ospf-enabled = yes
admin> set ospf-if-config-error-enabled = yes
admin> set ospf-if-auth-failure-enabled = yes
admin> write
TRAP/monitor-ospf written
```

Typical uses of traps and trap classes

If `alarm-enabled` is set to `yes`, the following commands cause the system to send trap PDUs when LIM redundancy takes effect, the secondary controller becomes primary, a DSL threshold is reached, and a PVC failure occurs. Note that the `alarm-enabled` parameter must be set to `yes` for the system to send these traps.

```
admin> set lim-sparing-enabled = yes
admin> set secondary-controller-state-change-enabled = yes
admin> set dsl-thresh-trap-enabled = yes
admin> set atm-pvc-failure-trap-enabled = yes
admin> write
TRAP test written
```

The following commands enable security class traps:

```
admin> set security-enabled = yes
admin> lim-sparing-enabled = yes
admin> write
TRAP test written
```

In the following example, the `host-name` value is used only as a profile index, not to locate the actual host on the network. A community name is specified, security-class traps are added to the default alarm-class traps, and this host receives a trap if the link fails.

```
admin> new trap
TRAP/"" read
admin> list
host-name* = ""
community-name = ""
host-address = 0.0.0.0
alarm-enabled = yes
security-enabled = no
port-enabled = no
slot-enabled = no
admin> set host-name = security-traps
```

```
admin> set community-name = Ascend
admin> set host-address = 10.2.3.4
admin> set security-enabled = yes
admin> set slot-enabled = yes
admin> write
TRAP/security-traps written
```

Because security traps and the `password-enabled` and `authentication-enabled` parameters are enabled, two traps are sent when either of the related conditions occur. The individual trap provides additional information about the specific event that triggered the trap.

Traps not belonging to any class

The `flashCardStateTrap` trap does not belong to a specific class. For the system to generate a trap whenever a flash card is removed or inserted from a control module, you need only to set the `ascend-flash-card-trap-enabled` parameter to `yes`.

How the system generates link-state traps for trunk ports

The system generates linkDown traps for the physical layer at boot-up for trunk modules, including E3-ATM, DS3-ATM, OC-3/STM-1, OC-12/STM-4 ports trunk ports, and T1 and E1 trunk ports *on the Stinger MRT*. The system generates a link down trap at boot time only for the physical layer of the trunk port. The system does not generate linkDown traps for LIM ports such as ADSL, SHDSL, and E1 and T1.

For the system to generate a linkDown trap for a trunk port, the following must be true:

- The trunk port must be enabled.
- Link state traps are enabled for this port, that is, in the `admin-state-phys-if` and `admin-perm-state-if` profiles.
- A trunk module or TRAM is installed in the Stinger chassis.
- Linkdown and Linkup traps are enabled in `trap` profile for this trap destination.

The system creates two profiles for each port present on the system: `admin-state-phys-if` profile for the physical layer and `admin-state-perm-if` for ATM layer.

The `admin-state-phys-if:desired-trap-state` parameter controls the generation of link-state traps for the physical layer and the `admin-state-perm-if:desired-trap-state` controls the generation of link-state traps for the ATM layer.

The default value `system-defined` for the `desired-trap-state` parameter has the following effects on link-state trap generation:

- With the default setting of `system-defined` for the `desired-trap-state` parameter in the `admin-state-phys-if` profile, the setting of the `link-phys-trap-state` parameter in the `system` profile specifies whether the system generates linkDown or link Up traps.
- With the default setting of `system-defined` for the `desired-trap-state` parameter in the `admin-state-perm-if` profile, the setting of the

`link-perm-trap-state` parameter in the `system` profile specifies whether the system generates linkDown or link Up traps.

The definition of the parameters in the `system` profile is as follows:

Parameter	Description
`system:link-phys-trap-state`	Enables/disables the generation of linkUp or linkDown traps if `the desired-trap-state` parameter in `admin-state-phys-if` profile is set to `system-defined`. With the default setting of `trap-state-enabled`, the system generates linkUp or linkDown traps for the physical interfaces. Specify `trap-state-disabled` to configure the system *not* to generate linkUp or linkDown traps for physical interfaces.
`system:link-perm-trap-state`	Enables/disables the generation of ATM layer linkUp or linkDown traps if `the desired-trap-state` parameter in `admin-state-perm-if` profile is set to `system-defined`. With the default setting of `trap-state-enabled`, the system generates linkUp or linkDown traps for ATM interfaces. Specify `trap-state-disabled` to configure the system *not* to generate linkUp or linkDown traps for ATM interfaces.

Configuring trap sequencing and heartbeat traps

Traps, like any other SNMP protocol data unit (PDU), use User Datagram Protocol (UDP) for transport. UDP by its nature does not guarantee delivery. In certain situations of network congestion and link failures, traps sent from a Stinger unit might be lost in transit and never reach the target element management system (EMS). Given the critical administrative dependence on trap delivery, any loss might result in delay of servicing outages.

Trap sequencing and the heartbeat trap

You can configure a Stinger unit to add sequence numbers to traps. With the trap sequencing feature enabled, the Stinger unit increments the trap sequence number before sending it, which provides a means for the NavisAccess® management software to detect if any trap was lost in transit.

NavisAccess® management software implements a sliding window to receive traps from each Stinger unit. This mechanism is necessary because UDP-based transport does not guarantee delivery of datagrams in sequence. For NavisAccess® management software to detect any missing traps, you can configure the Stinger unit to send a special heartbeat trap after a specified interval of trap inactivity.

When the Stinger unit generates a heartbeat trap, it does not increment the sequence number. Instead, it numbers heartbeat traps with the same sequence number as the last nonheartbeat trap sent. The Stinger unit does not save heartbeat traps in its notification log MIB.

If the NavisAccess® management software detects a gap in trap sequence number, it can take corrective action by requesting for a replay of the range of missing traps. The traps are replayed using the notification log MIB and its extension. Therefore, for this

feature to work, you must also enable the notification log on the Stinger unit (the `notify-log-enabled` parameter must be set to `yes`).

Configuring trap sequencing and the sending of heartbeat traps

To configure trap sequencing and the sending of heartbeat traps, create a new `trap` profile and name it `navisnlm`. For example:

```
admin> new trap navisnlm
TRAP/navisnlm read
```

The following parameters in the `trap` profile configure a Stinger unit to number traps sequentially and generate a heartbeat trap. [in TRAP/navisnlm]

```
...
notification-log-enable = no
notification-log-limit = 50
...
trap-sequencing = yes
heart-beat-trap-interval = 5
...
heart-beat-trap-enabled = no
```

Parameter	Description
`notification-log-enable`	Specifies whether SNMP traps (notifications) for this profile are logged. Specify `yes` to enable logging or `no` (the default) to disable it.
`notification-log-limit`	Maximum number of notification entries that can be held in the SNMP notification log. Specify a number from 1 to 500. The default is 50.
`trap-sequencing`	Enables/disables the Stinger unit from embedding sequence numbers in traps. NavisAccess® management software uses the trap sequence numbers to detect lost traps. By default, the Stinger unit does not embed sequence numbers in traps. Specify `yes` to enable this feature. For trap sequencing to work, the notification log must also be enabled (that is, the `notification-log-enable` parameter must be set to `yes`).
`heart-beat-trap-enabled`	Enables/disables the Stinger unit to generate heartbeat traps after a period of trap inactivity. By default, the Stinger unit does not generate a heartbeat trap during periods of trap inactivity. For the system to generate a heartbeat trap after a specified interval of trap inactivity specified by the `heart-beat-trap-interval` parameter, specify `yes`. The sequence number for a heartbeat trap is the same as the number of the last nonheartbeat trap generated by the Stinger unit.
`heart-beat-trap-interval`	Time elapsed, in minutes, since the the Stinger unit last generated a trap before it sends a heartbeat trap. Specify a value from 1 through 60. The default value is 5.

Sample configuration

The following sample commands configure the Stinger unit to generate traps with sequence numbers and to generate a heartbeat trap 10 minutes after it last sends a trap.

```
admin> new trap navisnlm
TRAP/navisnlm read
admin> set trap-sequencing = yes
admin> set notification-log-enable = yes
admin> set heart-beat-trap-enabled = yes
admin> set heart-beat-trap-interval = 10
admin> write
TRAP/navisnlm written
```

Displaying information about notification logs

The `nlmstat` debug command shows information about notification logs for a Stinger unit. The `nlmstat` command is available only in the debug environment. Its syntax is as follows, where ***trap*** is the name of a `trap` profile:

`nlmstat` [***trap***]

Without any arguments, the output of the `nlmstat` command reports is as follows. Table 9-7 describes the fields reported by the output of the `nlmstat` command.

```
admin> nlmstat
       Log Name                  Limit Logged     Bumped     #Replays   Replay
-------------------------------------------------------------------------------
navisnlm                          50   17         0          0          Idle
135.254.196.31                     50   20         0          0          Idle
```

Table 9-7. Description of fields for the output of the `nlmstat` command

Field	Specifies
`Log Name`	Name of the `trap` profile (EMS) .
`Limit`	Maximum number of trap notification entries that can be held in `nlm` log table for this named log. The value of `Limit` is the same as the value of `notification-log-limit` parameter in the `trap` profile.
`Logged`	Number of notifications logged by the Stinger unit for the `trap` profile.
`Bumped`	Number of log entries discarded to make room for a new entry when the total number of entries has exceeded the configured limit specified in the `trap` profile.
`#Replays`	Number of notifications that have been replayed for this log.
`Replay`	Status of the replay function. Indicates whether replay is active (`active`) or not (`idle`).

To display information about traps logged for a specific `trap` profile, enter the `nlmstat` command with the name of that `trap` profile. For example:

```
admin> nlmstat 135.254.196.31
 Notification Log Name  : 135.254.196.31
 Log Limit              : 50
 Notifications Logged   : 20
 Notifications Bumped   : 0
 Notifications Replayed : 0

 Index      Uptime     Gen-trap Spec-trap Version
 ------------------------------------------------
 1          0            0        0         V1
 2          0            6        48        V1
 3          0            6        12        V1
 4          400          3        0         V1
 5          400          3        0         V1
 6          400          3        0         V1
 7          400          3        0         V1
 8          400          3        0         V1
 9          400          3        0         V1
 10         400          3        0         V1
 11         400          3        0         V1
 12         0            3        0         V1
 13         0            6        26        V1
 14         100          6        35        V1
 15         100          6        35        V1
 16         100          6        35        V1
 17         300          6        12        V1
 18         600          6        12        V1
 19         1800         3        0         V1
 20         1800         3        0         V1
```

Table 9-8 defines the fields reported by the *`nlmstat trap`* command, in addition to the fields already defined in Table 9-7.

Table 9-8. Additional fields reported by the `nlmstat Ipaddress` command

Field	Specifies
`Index`	Index of a notification in `nlm` log table.
`Uptime`	System uptime, when the notification was generated.
`Gen-trap`	Generic trap type.
`Spec-trap`	Specific trap type.
`Version`	Trap version. Reported values can be `v1` (SNMPv1) or `v3` (SNMPv3).

Configuring SNMP watchdogs

An SNMP *watchdog* is a software routine that monitors the status of a particular aspect of a Stinger unit—for example, the temperature of a module. You can specify a watchdog name, and enable or disable the warning trap for each individual watchdog, by means of the TAOS command-line interface or SNMP. Once configured, the settings persist across system resets.

The system creates the `watchdog-config` profiles and ignores any user-created `watchdog-config` profiles. Each `watchdog-config` profile is identified by an index of the format {*type location unit-identifier*}. To list the watchdog routines available for your unit, use the `dir` command. For example:

```
admin> dir watchdog-config

28  11/19/2001 23:26:39  { fan fantray 1 }
28  11/19/2001 23:26:39  { fan fantray 2 }
28  11/19/2001 23:26:39  { fan fantray 3 }
36  11/19/2001 23:26:46  { relay cm-input-relay 1 }
36  11/19/2001 23:26:46  { relay cm-input-relay 2 }
36  11/19/2001 23:26:46  { relay cm-input-relay 3 }
36  11/19/2001 23:26:46  { relay cm-input-relay 4 }
36  11/19/2001 23:26:46  { relay cm-input-relay 5 }
36  11/19/2001 23:26:46  { relay cm-input-relay 6 }
36  11/19/2001 23:26:46  { relay cm-input-relay 7 }
34  11/19/2001 23:26:41  { cbus shelf-controller 0 }
```

To display the contents of the `watchdog-config` profile that the unit created for one of its fans, proceed as follows:

```
admin> read watchdog {fan fantray 1}
WATCHDOG-CONFIG/{ fan fantray 1 } read

admin> list
[in WATCHDOG-CONFIG/{ fan fantray 1 }]
watchdog-index* = { fan fantray 1 }
watchdog-trap-enable = yes
watchdog-name = "Stinger 10 Fan"
```

Parameter	Setting
`watchdog-index`	Watchdog type, location identification, and unit number of the watchdog. This parameter is read-only.
`watchdog-trap`	With the default `yes` setting, the system generates a trap for a watchdog routine. Specify `no` to disable the system from generating a trap for a watchdog routine.
`watchdog-name`	Name of an SNMP watchdog routine—up to 80 characters. By default, the system assigns a standard name. The value of the `watchdog-name` parameter is sent to the SNMP manager when the watchdog event causes a trap.

Managing SNMP interfaces

The Stinger unit supports the Interface MIB based on RFC 2233, which supersedes the `interfaces` group of the SNMP MIB-II, defined in RFC 1213. The interface table contains only the system's physical interfaces and dedicated (nailed) interfaces.

The SNMP index value of an interface does not change following a system reset. Moreover, if an entry is removed from the interface table dynamically, its index value is not reused until the management station has been reinitialized. The interface table does not contain virtual circuit interfaces, such as a frame relay data link configured on a channelized DS1 interface.

Verifying SNMP state

The Stinger unit allocates SNMP interfaces when it initializes a module for the first time. Because `admin-state` profiles are stored in NVRAM to retain state information during system resets, a physical device keeps the same SNMP interface number when the system resets or a power failure occurs.

Each physical interface in the system has an associated `admin-state-phys-if` profile, and each dedicated (nailed) connection has an associated `admin-state-perm-if` profile. These profiles store the object's desired state and SNMP interface number.

At system startup, the Stinger unit reads the `admin-state` profiles. If the addressed device is not present in the system and has been replaced by a device of another type, the Stinger unit deletes that profile and creates a new one, with a new SNMP interface number. However, the previous device's SNMP interface number does not become available until next time the system is reset or power to the unit is turned off and then turned back on, the old device's SNMP interface number becomes available for reassignment. Removing a module does not free up interface numbers. When you reinstall the module, the same interface number is assigned.

Using the `admin-state-perm-if` profile

The `admin-state-perm-if` profile holds information about Stinger unit nailed interfaces. The system creates a profile for an active nailed interface and assigns it an interface index. For example:

```
admin> dir admin-state-perm
    20  06/10/1999 14:25:32  con4-1
    20  06/10/1999 14:25:32  con4-2
    20  06/10/1999 14:25:32  con4-3
    20  06/10/1999 14:25:32  con4-4
    20  06/10/1999 14:25:32  con4-5
```

The `admin-state-perm-if` profile contains the following parameters, shown with sample values:

```
[in ADMIN-STATE-PERM-IF/con4-1]
station* = con4-1
snmp-interface = 28
desired-state = admin-state-up
```

```
desired-trap-state = trap-state-enabled
inet-profile-type = 1
```

Parameter	Setting
`station`	Name of a nailed profile, which can be a local `connection` profile or a RADIUS profile.
`snmp-interface`	Interface table index assigned to the nailed interface whose state is stored in this profile. The system assigns a numeric value.
`desired-state`	Desired administrative state of the addressed device. The system sets this parameter to `admin-state-down` if you disable this device, or to `admin-state-up` if you attempt to enable the device in normal operations mode. You can change the administrative state by using SNMP `set` commands, or the `slot` or `if-admin` commands.
`desired-trap-state`	Enable/disable link state traps for the interface. The system sets this parameter to `trap-state-enabled` if you specify that traps are to be generated for the interface, or to `trap-state-disabled` if an operator specifies that traps are not to be generated for the interface.
`inet-profile-type`	Whether the nailed profile is a local profile (0) or a RADIUS profile (1).

Using the `admin-state-phys-if` profile

The `admin-state-phys-if` profile holds information about the system's physical interfaces. For example:

```
admin> dir admin-state-phys
    24  04/17/2003 13:35:11  { shelf-1 slot-2 1 }
    24  04/17/2003 13:35:11  { shelf-1 slot-2 2 }
    24  04/17/2003 13:35:11  { shelf-1 slot-2 3 }
    ...
    ...
    ...
    25  04/17/2003 13:35:21  { shelf-1 slot-7 70 }
    25  04/17/2003 13:35:21  { shelf-1 slot-7 71 }
    25  04/17/2003 13:35:21  { shelf-1 slot-7 72 }
    25  04/17/2003 13:19:25  { shelf-1 first-control-module 32768 }
    24  04/17/2003 13:19:25  { shelf-1 first-control-module 1 }
    25  04/17/2003 13:19:25  { shelf-1 first-control-module 32769 }
    24  04/17/2003 13:19:25  { shelf-1 first-control-module 2 }
    25  04/17/2003 13:19:25  { shelf-1 first-control-module 32770 }
    24  04/17/2003 13:19:25  { shelf-1 first-control-module 3 }
    25  04/17/2003 13:19:25  { shelf-1 first-control-module 32771 }
    25  04/17/2003 13:19:25  { shelf-1 first-control-module 32772 }
    25  04/17/2003 13:19:25  { shelf-1 first-control-module 32773 }
    26  04/17/2003 14:19:42  { shelf-1 first-control-module 32774 }
    25  04/17/2003 13:19:25  { shelf-1 first-control-module 32775 }
    ...
```

```
...
...
25  04/17/2003 13:19:26  { shelf-1 slot-16 22 }
25  04/17/2003 13:19:26  { shelf-1 slot-16 23 }
25  04/17/2003 13:19:26  { shelf-1 slot-16 24 }
24  04/17/2003 13:35:10  { shelf-1 trunk-module-1 1 }
24  04/17/2003 13:35:10  { shelf-1 trunk-module-1 2 }
24  04/17/2003 13:35:10  { shelf-1 trunk-module-2 1 }
24  04/23/2003 22:52:02  { shelf-1 trunk-module-2 2 }
24  04/17/2003 13:19:25  { shelf-1 trunk-module-2 3 }
24  04/17/2003 13:19:25  { shelf-1 trunk-module-2 4 }
24  04/17/2003 13:19:25  { shelf-1 trunk-module-2 5 }
24  04/23/2003 21:03:28  { shelf-1 trunk-module-2 6 }
```

The Stinger unit creates a profile for each of its physical interfaces. The `admin-state-phys-if` profile contains the following parameters, shown here with sample values:

```
[in ADMIN-STATE-PHYS-IF/{ shelf-1 slot-4 1 }]
device-address* = { shelf-1 slot-4 1 }
slot-type = al-dmtadsl-atm-card
snmp-interface = 4
modem-table-index = 0
desired-state = admin-state-up
desired-trap-state = trap-state-enabled
```

Parameter	Setting
`device-address`	Physical slot address within the system.
`slot-type`	Type of module at that address.
`snmp-interface`	Interface table index assigned to the device whose state is stored in this profile. The system assigns a numeric value, which does not change as long as the interface is present in the system. If you remove the module and or delete its profiles, (for example, through the use of a `slot -r` command), the index number is freed for future use.
`modem-table-index`	Modem table index assigned to the device whose state is stored in this profile. The system assigns a numeric value. Because the Stinger unit does not support modems, the value is always 0.
`desired-state`	Desired administrative state of the addressed device. The system sets this parameter to `admin-state-down` if you disable the device or to `admin-state-up` if you attempt to enable the device in normal operations mode. You can change the administrative state by using SNMP `set` commands or the `slot` or `if-admin` commands.

Parameter	Setting
`desired-trap-state`	Desired `linkUp-linkDown` trap state of the interface. The system sets this parameter to `trap-state-enabled` if you specify that linkUp and link Down traps are generated for the interface, or to `trap-state-disabled` if you specify that link Up and link Down traps are not generated for the interface.

Viewing SNMP interface numbers

To display SNMP interface numbers, use the `if-admin` command. To see a list of available SNMP interface numbers, use the `-a` option:

```
admin> if-admin -a
Available SNMP interface numbers
        95 - 142
       391 - 404
       414 - 448
       589 - infinity
```

To see a list of all SNMP interface numbers assigned by the system, use the `-l` option:

```
admin> if-admin -l
 SNMP-IF   DEVICE ADDRESS   STATUS
     1   -   {  1  9  1 }     active
     2   -   {  1  9  4 }     active
     3   -   {  1  9 32768 }     active
     4   -   {  1  9 32769 }     active
     5   -   {  1  9 32770 }     active
     6   -   {  1  9 32771 }     active
     7   -   {  1  9 32772 }     active
     8   -   {  1  9 32773 }     active
     9   -   {  1  9  2 }     active
    10   -   {  1  9 32775 }     active
    11   -   {  1  9  3 }     active
    12   -   { ATM-IF:2449 }     active
    13   -   {  1 17  1 }     active
    14   -   {  1 17  2 }     active
    15   -   { ATM-IF:801 }     active
    16   -   { ATM-IF:802 }     active
    17   -   {  1 18  1 }     active
    18   -   {  1 18  2 }     active
    19   -   {  1 18  3 }     active
    20   -   {  1 18  4 }     active
    21   -   {  1 18  5 }     active
    22   -   {  1 18  6 }     active
    ..
```

Initiating interface state changes

To enable or disable an SNMP interface, use the `if-admin` command with the `-d` option, and specify the interface number. For example:

```
admin> if-admin -d 2
interface 2 state change forced
```

To reenable a disabled device, use the `if-admin` command with the `-u` option, and specify the interface number. For example:

```
admin> if-admin -u 2
interface 2 state change forced
```

Resetting the SNMP interface table sequentially

By default, the SNMP interface table is built as modules are installed in the Stinger unit. The `if-admin` command `-r` option enables you to reset the order of the table to be sequential based on slot number. For example:

```
admin> if-admin -r
SNMP interface mappings reset.
Reset system in order to take effect.
```

You must reset the Stinger unit for the new order to take effect.

Note If the `if-admin -r` command fails, reenter it. If the command fails a second time, disable all modules with the `slot -d` command, remove the configuration from all modules by using `slot -r`, reset the system, and run the `if-admin -r` command again.

Naming convention for SNMP-configured profiles

To configure an ATM circuit via SNMP, you create an entry in the virtual circuit cross-connect table if the two virtual links are virtual channel links (VCLs), or in the virtual path cross-connect table if the links are virtual path links (VPLs). A cross-connect entry identifies its two ATM interfaces by `ifIndex` value. The two sides of the circuit are distinguished as the high `ifIndex` (the interface with a higher number in the `ifTable`, such as 25) and the low `ifIndex` (the interface with a lower number in the `ifTable`, such as 5).

For example, the following sample entry shows `ifIndexA` and `ifIndexB` as the low and high `ifIndex` values for a cross-connect:

```
atmVcCrossConnectIndex              = entry-index
atmVcCrossConnectLowIfIndex         = ifIndexA
atmVcCrossConnectLowVpi             = VpiA
atmVcCrossConnectLowVci             = VciA
atmVcCrossConnectHighIfIndex        = ifIndexB
atmVcCrossConnectHighVpi            = VpiB
atmVcCrossConnectHighVci            = VciB
atmVcCrossConnectAdminStatus        = down
atmVcCrossConnectRowStatus          = createAndGo
```

Default naming convention

For each cross-connect entry you create via SNMP, the system creates a `connection` profile and assigns the profile a name that specifies the slot and port with the low `ifIndex` value first, followed by the slot and port with the higher `ifIndex` value. Following is the format of this naming convention:

low interface index slot **:** *port-vpi-vci* **x** *high interface index slot* **:** *port-vpi-vci*

For example, the following listing shows two LIM-to-trunk cross-connects from slot 1 to slot 17, created via SNMP:

```
admin> dir connection
147  11/25/2001 18:28:05  17:1-0-50x1:1-0-50
146  11/25/2001 18:36:25  17:1-15x1:1-15
```

Configurable naming convention

You can configure the system to use command-interface identifiers instead of the low and high interface indexes in the SNMP ifTable. When command-interface identifiers are configured and you create a cross-connect entry via SNMP, the system creates a `connection` profile and assigns the profile a name that specifies the slot and port of the first side of the ATM circuit (the interface specified in the `connection atm-options` subprofile), followed by the slot and port of the second side of the ATM circuit (the interface specified in the `atm-connect-options` subprofile). Following is the syntax of the new configurable naming convention:

atm-options-if-slot **:***port-vpi-vci***x***atm-connect-options-if-slot* **:***port-vpi-vci*

For example, the following listing shows two LIM-to-trunk cross-connects created via SNMP:

```
admin> dir connection
147  11/25/2001 18:28:05  1:1-0-50x17:1-0-50
146  11/25/2001 18:36:25  1:1-15x17:1-15
```

Selecting the naming convention for `connection` profiles

Following is the parameter, shown with its default value, for configuring the naming convention for `connection` profiles:

```
[in SYSTEM]
connection-profile-auto-naming-convention = lower-interface-number-first
```

Using Debug Commands

A

Note Every attempt has been made to confirm that this chapter correctly describes the functionality and output of the Stinger debug commands. However, although debug mode can be a very valuable troubleshooting tool for anyone, its primary focus is on the requirements of Lucent Technologies development engineers. For this reason, Lucent does not guarantee the completeness of the list of debug commands published for a given release, or descriptions of their functionality.

Caution Under most circumstances, debug commands are not required for correct operation of a Stinger unit. Under some circumstances, these commands might produce undesirable results. Use the following information with caution. Contact Lucent OnLine Customer Support at `http://www.lucent.com/support` with any questions or concerns.

Enabling debug permissions

Before you can access the debug commands, you must log into the Stinger unit with a `user` profile that specifies debug privileges.

To enable debugging privileges:

1 Open a `user` profile:

```
admin> read user admin
```

2 Enable debug permissions:

```
admin> set allow-debug = yes
```

This is a hidden parameter. It does not appear in the interface.

3 Write the profile to save the changes:

```
admin> write
```

Note When you are logged into a Stinger unit with debug privileges, the interface might display normally unavailable parameters and commands, some of which are not configurable in certain situations. Therefore, Lucent Technologies recommends that you create a special profile for debugging purposes, and use that profile only when you are debugging the Stinger unit.

Enabling debug output

To enable debug output for all commands on the system or on a module, use the `debug` command as in the following examples.

To enable debug output:

```
admin> debug on
Diagnostic output enabled
```

To disable debug output:

```
admin> debug off
Diagnostic output disabled
```

When you enable debug output, the Stinger unit displays the debug messages on the terminal screen.

Setting debug levels

Debug levels vary depending on the command. But generally, the lower you set the debug level, the fewer messages the Stinger unit displays. Setting the debug level to `0` (zero) disables the debug output for the command.

Set the debug level with the `-t` toggle option, as in the following examples:

```
admin> ifmgr -t 0
ifmgr debug level is now 0 (disabled)
admin> ifmgr -t 4
ifmgr debug level is now 4 (enabled)
```

Getting online help for debug commands

To see a list of all commands, including the debug commands, enter a question mark (`?`) at the command prompt, as in the following example:

```
admin> ?
?                              ( user )
 acct-failsafe                  ( debug )
 agereCfg                       ( debug )
 agereFpga                      ( debug )
 agrm                           ( debug )
 agsh                           ( debug )
 alarm                          ( system )
 aliasTable                     ( debug )
 annexType                      ( debug )
```

```
 apsMgr                          ( debug )
 arptable                        ( system )
 asiramtest                      ( debug )
 atmcacstat                      ( debug )
 atmCacToggle                    ( debug )
 atmCktState                     ( debug )
 atmConnectionFailures           ( system )
 atmControlState                 ( debug )
 atmDelGet                       ( debug )
 atmds3trunkdev                  ( debug )
 atme3trunkdev                   ( debug )
 atmems                          ( debug )
 AtmEmsDebug                     ( debug )
 atmFlexVpiVci                   ( debug )
 atmGet                          ( debug )
 atmInternalLines                ( system )
 atmnbase                        ( debug )
 atmNbaseDbg                     ( debug )
 atmoc3trunkdev                  ( debug )
 atmPvcState                     ( debug )
 atmqos                          ( system )
 atmSet                          ( debug )
 atmsig                          ( system )
 atmstabds3trunk                 ( debug )
 atmstabe3trunk                  ( debug )
 atmstabima                      ( debug )
 atmstaboc3trunk                 ( debug )
 atmTest                         ( debug )
 atmtrunkmgr                     ( diagnostic )
 atmtrunkreset                   ( diagnostic )
 AtmTrunks                       ( system )
 atmTSet                         ( debug )
 atmvccmgr                       ( debug )
 atmvccstat                      ( system )
 atmvcl                          ( system )
 atmvcx                          ( system )
...
```

To get basic help for a debug command, enter the `help` command, followed by the name of the debug command, as in the following example:

```
admin> help ifmgr
ifmgr usage: ifmgr [-r <vRouterName>] -option
             -d  (d)isplay interface table entries.
             -d <ifNum>  (d)etails of given i/f table entry.
             -n <conn profile name> display slot and ifNum of conn.
       ifmgr [up|down] [ifNum|ifName]
```

Summary of common debug commands

Debug commands allow you to monitor and diagnose different areas of Stinger functionality. Table A-1 lists common debug commands. To use any of these commands, you must have debug permissions and the debug facility enabled. For

more information on debug permissions see "Enabling debug permissions" on page A-1. For more information on enabling the debug facility see "Enabling debug output" on page A-2.

Table A-1. Commonly used debug commands

Command	Section
`pools`	"Displaying memory pool information" on page A-5
`portinfo`	"Displaying Stinger port information" on page A-7
`telnetdrestart`	"Resetting TCP port 23" on page A-7
`revision`	"Displaying the serial numbers" on page A-8
`tsshow`	"Displaying system uptime and revision number" on page A-8
`update`	"Modifying Stinger unit functionality" on page A-8
`acct-failsafe`	"Using the acct-failsafe debug command" on page A-9
`radservdump`	"Verifying settings in the external-auth profile" on page A-10
`radsessdump`	"Displaying RADIUS accounting session status" on page A-10
`radstats`	"Displaying RADIUS accounting session status" on page A-10
`netif`	"Displaying network interface mappings" on page A-12
`eoc`	"Using the EOC command on ADSL interfaces" on page A-13
`controller-redundancy`	"Displaying the status of redundant control modules" on page A-15
`ifmgr`	"Displaying interface management information" on page A-16

System and devices debugging

The following sections describe the commands used for system and devices debugging.

Displaying memory pool information

The pools debug command displays a snapshot of a large selection of memory pools, the size of each pool, and the status of each pool. At the end of the list is a summary of the total memory allocation in the Stinger.

Memory is dynamically allocated to support various tasks, and is normally freed when a particular task has been completed. Taking pools snapshots over an extended period of time can help troubleshoot a memory leak problem, in which memory is allocated for a task but never freed.

Snapshots of a normal system never show the entire quantity of allocated memory (or even any single pool) increasing over an extended period of time.

The displayed output of the pools command is usually very large. The following example displays just a portion of the typical output:

```
admin> pools
Pool Name                       size limit   inUse  InUseSize   hiWat  free
AcctEvnt                          20     0       3        112       3     0
AcctStateChgRegn                   8     0       1         16       1     0
ActiveTrunkWanSessPool            16     0       0          0       1     0
alarmtask Mail msg pool           64     0       0          0      15     0
ambStubReqInfo                    20     0       0          0       1     9
arg                             1020     0       0          0       1     0
arpcache                          60     0       1         64       4     0
ATM DCL-CALL Cb Pool             324     0       1        336       2  2998
ATM PvcMgrMsg Pool                84     0       0          0       3   127
ATM SPVC-EMS Mail Pool            40     0       0          0       6    95
ATM-EMS Mail Pool                 24     0       0          0      97    97
ATM-EMS Port Entry Pool          108     0     236      26512     236     0
ATM-NBASE                      10028     0     167    1675344     167   232
ATM-NBASE-VAR                   6488     0       5      40000       5     0
ATM-Trunk Call Block             100  2000       0          0       1  1999
atm1483Internal                   16     0       0          0       1     0
...
...
...
vRouterBlock                    2768     0       2       5536       2     0
vRouterHash                        8     0       4         64       4     0
XkAttributeContainer             152     0      16       2560      16     0
XkMsg                            168     0      16       2816      91    75
XkMsg CloneNode                   44     0      16        768      16     0
XkMsg LARGE PageNode             428     0      16       6912      76    59
XkMsg LoanNode                    56     0      16       1024      16     0
XkMsg MEDIUM PageNode            300     0      16       4864      16     0
XkMsg SMALL PageNode             172     0      16       2816      16     0
XkMsg XLARGE PageNode            556     0      16       8960      61    45
_buffPool                        104     0       0          0      26     0
_buffPool                        104     0       0          0      15     0
_oamMsgPool                       16     0       1         16       2     0
_tntCallMsgPool                 2408     0       0          0       2     0

                  total pools:          350
          total buffers in use:         8950
```

```
                total malloc's:    574276459
            total freelist gets:     74144880
                total memfree's:    574207570
            total freelist puts:     74161950
                malloc failures:            0
               memfree failures:            0

          number of busy blocks:        68885
          number of free blocks:          282
    total bytes busy in vmHeap:     34527312
           free bytes in pools:      4480032
          free bytes in vmHeap:     71724480
            largest busy piece:      4773392
            largest free piece:     71715520
            number of segments:            2
          total memory - vmHeap:    107358560
          total memory - vpools:    107358432
```

The first portion of the pools command output includes the following fields:

Field	Indicates
`Pool Name`	Pool name.
`size`	Size of the pool, in kilobytes.
`limit`	Maximum number of buffers that can be allocated to a pool.
`inuse`	Number of pools in use.
`hiwat`	Highest number of pools allocated to a task since the Stinger started operating.
`heapadrs`	Memory address of the pool.

The latter portion of the command output shows memory usage information. Following are descriptions of some of the more important fields in this display:

Field	Indicates
`total pools`	Total number of pools in use.
`total buffers in use`	Number of buffers in use.
`total memalloc`	Total number of times the Stinger allocated a block of memory for use.
`total memfree`	Total number of times the Stinger freed a block of memory. Normally, this field is close in value to `total memalloc`.
`memalloc in use`	Total number of memory pools in use. This value is the difference between the total number allocated and total number freed.

Field	Indicates
memalloc failures	Total number of times the Stinger failed to allocate a block of memory for use.
memfree failures	Total number of times the Stinger failed to free a block of memory.
memalloc high water	Highest number of memory pools in use at any one time.

Displaying Stinger port information

The portinfo debug command displays information about the Stinger ports.

The portinfo debug command uses the following syntax:

portinfo *port-number*

For example, the following command displays port statistics for slot 1:

```
admin> show
Controller { second-control-module } ( PRIMARY ):
                                  Reqd  Oper   Slot Type
    { shelf-1 slot-2 0 }          UP    UP     terminator-card
    { shelf-1 slot-3 0 }          UP    UP     glite-atm-48-card
    { shelf-1 slot-4 0 }          UP    UP     ima-24t1-card
    { shelf-1 slot-5 0 }          UP    UP     dadsl-atm-24-card
    { shelf-1 slot-6 0 }          UP    UP     ima-8-t1-card
    { shelf-1 slot-11 0 }         UP    UP     stngr-48a-adsl-card
    { shelf-1 slot-12 0 }         UP    UP     shdsl-card
    { shelf-1 trunk-module-1 0 } UP    UP     oc3-atm-trunk-daughter-card
   { shelf-1 trunk-module-2 0 } UP    UP    2oc3-4ds3-atm-trunk-daughter-card
admin> portinfo 5
Printing fixed/allocated ports for slot 5
Linear Port:   7010
- fixed:       FALSE
- relative s#: 5
- relative p#: 2
- paired port: 65535
- slave:       FALSE
- physical:    FALSE
```

Resetting TCP port 23

The telnetdrestart command restarts the TCP daemon service and reopens listening port 23 when the port is closed. The syntax of the telnetdrestart command is as follows:

telnetdrestart -[r]

The -r option restarts TCP port 23. To display command usage, enter telnetdrestart without any options.

The following sample command restarts disabled port 23:

```
admin> telnetdrestart -r
The server has been restarted.
```

If you enter the command when the port is already open, the system generates the following message:

```
The telnet server port is already up
```

Displaying the serial numbers

The `revision` debug command displays the serial number of the Stinger unit. To use the command, proceed as in the following example.

In the output, `10539207` is the serial number of the Stinger unit.

```
admin> revision
first-control-module : revision =  C 1 10 10539207
```

Displaying system uptime and revision number

The `tsshow` debug command displays uptime and revision information about the Stinger unit.

The `tsshow` debug command uses the following syntax:

```
tsshow [?] [uptime] [revision]
```

Syntax element	Description
`?`	Lists all options.
`uptime`	Displays system uptime.
`revision`	Displays the software and version currently running.

Following are some samples of `tsshow` output:

```
admin> tsshow uptime
system uptime: up 36 days, 9 hours, 59 minutes, 27 seconds
```

```
admin> tsshow revision
system revision:  stngrcm2 9.5-206
```

Modifying Stinger unit functionality

The `update` debug command modifies optional functionality of the Stinger unit. To enable some options, you must obtain one or more software licenses (supplied by a Lucent representative) that enable the functionality in your Stinger. After each string is entered, the word *complete* appears, indicating that the Stinger accepted the license.

If you enter `update` without a text string modifier, the Stinger unit displays a list of current configuration information, as shown in the following example:

```
admin> update
Host interfaces: 4
Net interfaces: 0
Field features 1: 0
Field features 2: 32
```

```
Field features 3: 0
Field features 4: 28
Protocols: 2048
New Options 1: 6
New Options 2: 0
New Options 3: 0
New Options 4: 0
New Options 5: 0
New Options 6: 9729
New Options 7: 40
```

Suppose you enter `update` with a text string modifier as shown:

```
admin> update 5 1023 12321312312312321
```

The following two messages indicate that the text strings were entered incorrectly:

```
update command: invalid arg 3!
update command: disallowed
```

RADIUS debugging

The following sections describe the commands that you use for RADIUS debugging. For information about RADIUS, see the *TAOS RADIUS Guide and Reference*.

Using the `acct-failsafe` debug command

The `acct-failsafe` debug command is available on the primary control module and LIMs for verifying correct accounting proxying. (LIMs do not include the `-d` option.)

This command has the following syntax:

```
acct-failsafe -d [shelf slot] -t -?
```

Syntax element	Description
`-d`	Displays account fail-safe (AFS) information for a particular slot or, with no arguments, for all slots. This option is available only on the Stinger primary control module.
`-t`	Toggles the module debug level.
`-?`	Displays the command summary.

To display information about the calls on any slot that are candidates for proxy accounting, enter the following command:

```
admin> acct-failsafe -d
Slot 1/8:
HashTable @ 10542160, bucketCount: 192, callCount: 23, hashName <afs-1:8>
Slot 2/5:
HashTable @ 10585730, bucketCount: 48, callCount: 7, hashName <afs-2:5>
```

The following sample command displays the same information for a single module in shelf 1, slot 8:

```
admin> acct-failsafe -d 1 8
Slot 1/8:
HashTable @ 10542160, bucketCount: 192, callCount: 23, hashName <afs-1:8>
```

To specify which level of debug to use for the command, use the -t option. A debug level of zero indicates none (no messages). A level of 7 is fairly verbose.

Verifying settings in the external-auth profile

Use the radservdump command to verify the configuration you have set in the external-auth profile.

To enable radservdump debugging, enter radservdump at the command prompt as follows:

```
admin> radservdump
RADSERVDUMP debug display is ON
```

This command does not display any information related to the configuration of either your RADIUS authentication server or your RADIUS accounting server.

As shown in the following example, a Stinger unit has been configured with two RADIUS servers, 1.1.1.1 and 2.2.2.2. The port has not been changed from its default of 1700.

```
admin> radservdump
Rad serv vars: port=1700,sockId=8
 0) clients=1010101
 1) clients=2020202
 2) clients=0
 3) clients=0
 4) clients=0
 5) clients=0
 6) clients=0
 7) clients=0
 8) clients=0
```

Displaying RADIUS accounting session status

The radsessdump debug command displays the state of all RADIUS accounting sessions.

To enable radsessdump debugging, enter radsessdump at the command prompt as shown in the following example:

```
admin> radsessdump
RadActSess:  state route sessID   nasPort authM  evTime
             loadd 00289 252365175 012032 local  523932
             loadd 00288 252365174 012032 local  523946
             loadd 00287 252365173 012032 local  523945
             loadd 00286 252365172 012032 local  523946
             loadd 00227 252355493 012032 local  370610
             loadd 00226 252355492 012032 local  370611
             loadd 00225 252355491 012032 local  370608
             loadd 00224 252355490 012032 local  370609
             loadd 00004 252332182 012032 none   29
             loadd 00003 252332181 012032 none   28
```

```
loadd 00002 252332180 012032 none   27
loadd 00001 252332179 012032 none   26
```

The radsessdump command displays the following information:

Field	Indicates
state	State of the RADIUS accounting parameters and any accounting requests that have been sent. This field reports one of the following values: ■ init—Initializing. No RADIUS accounting parameters have been loaded. ■ loadd—RADIUS accounting parameters have been loaded, but an accounting request either has not been issued or has failed. ■ start—All RADIUS accounting parameters are loaded. An accounting request has been issued. ■ done—Session is over. No accounting request was issued, or the request failed. ■ stop—Session is over. An accounting stop request has been issued.
route	Internal route ID.
sessid	Session ID. This setting depends on the route ID.
nasPort	Statistics about the call. The first two digits indicate the type of call: 1 indicates a digital call, 2 indicates an analog call. The next two digits indicate the line on which the call was received. The last two digits indicate the channel on which the call was received.
authM	Method of authentication.
evTime	Event time. This is a timestamp.

Displaying RADIUS authentication and accounting statistics

The radstats debug command displays a compilation of RADIUS authentication and accounting statistics.

To enable radstats debugging, enter radstats at the command prompt as shown:

```
admin> radstats
RADIUS authen stats:
```

In the following sample message, A denotes *Authentication*, and O denotes *Other*. There were 612 authentication requests sent and 612 authentication responses received:

```
0  sent[A,O]=[612,15], rcv[A,O]=[612,8]
```

Of connections attempts, 602 were authenticated successfully, and 18 were not:

```
timout[A,O]=[0,6], unexp=0, bad=18, authOK=602
```

In the next sample message, the IP address of the RADIUS server is 1.1.1.1, and the curServerFlag indicates whether or not this RADIUS server is the current

authentication server. (You can have several configured RADIUS servers, but only one is current at any one time.) 0 indicates *no*. 1 indicates *yes*.

```
IpAddress 1.1.1.1, curServerFlag 1
RADIUS accounting stats:
```

The next message indicates that the Stinger unit sent 1557 accounting packets and received 1555 responses (ACKs from the accounting server). Therefore, the unexp value is 2. This value does not necessarily indicate a problem, but might be the result of the Stinger unit timing out a particular session before receiving an ACK from the RADIUS server. A momentarily heavy traffic load might cause this condition. The value of bad is the number of packets that were formatted incorrectly by either the Stinger unit or the RADIUS server.

```
0  sent=1557, rcv=1555, timout=0, unexp=2, bad=0
```

In the next message, note that the accounting server is different from the authentication server. The accounting and authentication servers do not need to be running on the same host, although they can be.

```
IpAddress 2.2.2.2, curServerFlag 1
Local Rad Acct Stats:
```

You can use the next two messages to look for traffic congestion problems or badly formatted accounting packets. Under typical conditions, you might see a few packets whose acknowledgments fail.

- The following message indicates whether any RADIUS requests have been dropped by the Stinger unit. With this particular message, no requests were dropped and 1557 were sent successfully.

  ```
  nSent[OK,fail]=[1557,0], nRcv=1557, nDrop[QFull,Other]=[0,0]
  ```

- The following message indicates whether any session timeouts resulted from a failure to receive RADIUS responses. The message also indicates responses that are received by the Stinger unit but do not match any expected responses. The Stinger unit keeps a list of sent requests, and expects a response for each request. In the following message, one response was received from the RADIUS server that did not match any of the requests that the Stinger had sent out. This situation might be caused by a corrupted response packet, or by the Stinger unit timing out the session before the response was received.

  ```
  nRsp[TimOut,NoMatch]=[0,1], nBackoff[new,norsp]=[0,0]
  ```

The following messages display a summarized list of RADIUS server statistics.

```
Local Rad Serv Stats:
unkClient=0
index 0 #Sent = 0, #SendFail=0 badAuthRcv = 0, badPktRcv = 0
```

Interface debugging

The following sections describe the commands that you can use to debug Stinger interfaces.

Displaying network interface mappings

The netif debug command displays the Stinger network interface mappings. This command has the following syntax:

```
netif -m | -q | -v |?
```

Syntax element	Description
-m	Displays mappings for the specified map type.
-q	Displays the queue for a map.
-v	Displays valid mapping tables.
?	Displays the command summary.

The following example displays valid interface mappings:

```
admin> netif -v
map 0x1042C0E0: type 0 (call-id), id 0x1042B5A0
```

This example displays interface mappings that contain `type 0`:

```
admin> netif -m 0
SHELF       SLOT  SysID  SlotID
   1         1      52      2
   1         6      90     58
   1         6      89     57
   1         6      86     56
   1         6      78     51
   1         6      72     50
   1         6      71     49
   1         6      70     48
   1         6      69     47
   1         6      68     46
   1         6      62     45
   1         6      61     44
   .
   .
   .
```

Using the EOC command on ADSL interfaces

The `eoc` command allows you to send read and write requests to the standard register set, as defined in ANSI T1.413 Issue 2, ITU 992.1 and ITU 992.2, on the customer premises equipment (CPE) by way of the embedded operations channel (EOC). The ADSL interfaces on the following hardware support this command:

- 24-port ADSL LIM
- 48-port ADSL G.lite LIM
- 40-port ADSL Annex C LIM
- 48-port ADSL Annex A LIM
- 48-port ADSL Annex B LIM
- Stinger MRT unit with 36 ADSL ports
- 72-port ADSL Annex A LIM

You must first open a session with the LIM, or with logical slot 1 on a Stinger MRT to use this command. The `eoc` command has the following syntax:

```
eoc -p [-r|-w reg slot port [data]]
```

Syntax Element	Description
`-p`	Enable/disable module debug.
`-r`	Read from the specified register.
`-w`	Write to the specified register.
reg	Register number to read from or write to. With the read option, specify a value from 0 through 8 or 10. With the write option, specify 4 or 5.
slot	Slot number.
port	Port number.
data	Data to save to the register using the `-w` option. Enter up to 32 bytes of data.

The following sample commands display the output of the `eoc` command from a 48-port G.lite ADSL LIM:

```
admin> open 1 4

glite-atm-48-1/4> eoc -r 1 4 5
Eoc status: OK
Eoc Read Rev number of ATU-R -
0x0f 0x00 0x42 0x43 0x4c 0x41 0x00 0x00
0x01 0x00 0x22 0x01 0x01 0x00 0x00 0x00
0x03
```

The following example shows the output of the `eoc` command from a 48-port Annex A ADSL LIM:

```
admin> open 1 4

dadsl-atm-48a-1/6> eoc -r 1 6 1
Cmd Seq No - 00002
dadsl-atm-48a-1/6>
EOC READ, Port - 1, Reg - 1, Cmd Seq No. - 00002, Status - OK
0x21 0x03 0x00 0x00
```

Note Because different CPE devices respond at different rates, the system runs the command in the background and displays the results as they become available. As a result, the command prompt might sometimes appear in the middle of the output.

Control module debugging

The following sections describe the commands that you use for control module debugging. The *Stinger IP2000 Configuration Guide* also describes debug commands that are used specifically for the IP2000 control module.

Displaying the status of redundant control modules

The `controller-redundancy` debug command displays the status of the primary and secondary control modules in a Stinger unit with redundant control modules.

To enable `controller-redundancy` debugging, proceed as shown in the following example:

```
admin> controller-redundancy
My id                  = Slot 8  Controller-1
My state               = MONITORING
My function            = PRIMARY
Remote's state         = MONITORING
Remote's function      = SECONDARY
HW state               = I_AM_PRIMARY
Remote detected by HW = PRESENT_ACTIVE
Msgs sent              = 5279
Send errors            = 1
Msgs received          = 5279
State machine events = 6143
State transitions   = 2
Profile Xfer Cycles  = 11
Profile sends        = 161
Profile Rx Cycles    = 0
Profile Rx           = 0
_needProfileTransfer = 0
_remoteCntrlActive   = 1
_debug level         = 17
read slot serial #   = 9235004
```

Following are descriptions of some of the more important fields in this display:

Field	Indicates
My id	Location of the primary control module.

My state	State of the primary control module. Following are valid states:
	`Initial`
	`Load_context`
	`Start_POST`
	`Local_POST`
	`Remote_POST`
	`Selecting`
	`Selection_Complete`
	`Inauguration`
	`Primary_to_Operational`
	`Loading`
	`Secondary_to_Operational`
	`Monitoring`
	`Dead`

Field	Indicates

My function	Function of the primary control module. Following are valid functions:
	`No_Function`
	`Primary`
	`Secondary`

Remote's state	State of the secondary control module. See `My state` for valid values.
Remotes's function	Function of the secondary control module. See `My function` for valid values.

HW state	Hardware state of the primary control module. Following are valid hardware states:
	`No_Primary_Controller`
	`I_Am_Primary`
	`Other_Controller_Primary`
	`HW_Status_Not_Available`

Remote detected by HW	Condition of secondary control module hardware: `Present_Active.` Hardware is present and software is running. `Present_Inactive.` Hardware is present, but software is not running (for example, is being reset). `Not_Present`. Hardware is not present. `Unknown.` Cannot be determined.

Displaying interface management information

The `ifmgr` debug command displays interface-table entries, toggles the debug display, and marks an interface as enabled or disabled. You can enter this command only from the control module.

The `ifmgr` debug command uses the following syntax:

`ifmgr [-d [`*`ifnam`*`|`*`ifnum`*`]|-t] [up|down `*`ifnum`*`|`*`ifname`*`]`

Syntax element	Description
`-d`	Displays interface table entries.
`-d `*`ifname`*`|`*`ifnum`	Displays details of the specified interface name or number.
`-t`	Toggles the debug display.
`up|down `*`ifnum`*`|`*`ifname`	Enables or disables the specified interface. These options have the same effect as setting the `enabled` parameter in the `ethernet` profile, and are subject to the same limitations.

To display the interface table entries, use the **`-d`** option. (The `netstat` command also displays a hyphen to indicate a disabled Ethernet interface.) For example:

```
admin> ifmgr -d
bif slot sif u m p ifname      host-name  remote-addr       local-addr
-------------------------------------------------------------------------------
-
000 1:17 000 *     ie0        -          0.0.0.0/32        192.168.7.133/32
001 1:17 001 *     lo0        -          0.0.0.0/32        127.0.0.1/32
002 0:00 000 *     rj0        -          0.0.0.0/32        127.0.0.2/32
003 0:00 000 *     bh0        -          0.0.0.0/32        127.0.0.3/32
004 0:00 000 *     wanabe     -          0.0.0.0/32        127.0.0.3/32
005 0:00 000 *     local      -          0.0.0.0/32        127.0.0.1/32
006 0:00 000 *     mcast      -          0.0.0.0/32        224.0.0.0/32
007 0:00 000 -     tunnel7    -          0.0.0.0/32        192.168.7.133/32
008 1:11 001 *   p wan8       tnt-t1-t32 200.2.1.2/32      192.168.7.133/32
009 1:11 002 *   p wan9       tnt-t1-t32 200.2.2.2/32      192.168.7.133/32
010 1:11 003 *   p wan10      tnt-e1-t22 200.3.2.2/32      192.168.7.133/32
011 1:11 004 *   p wan11      tnt-e1-t32 200.5.1.2/32      192.168.7.133/32
012 1:11 005 *   p wan12      tnt-e1-t32 200.5.2.2/32      192.168.7.133/32
013 1:11 006 *   p wan13      tnt-t1-t22 200.1.1.2/32      192.168.7.133/32
014 1:15 001 *   p wan14      tnt-t1-s1- 100.1.100.2/32    100.6.100.2/32
015 1:11 007 *   p wan15      tnt-e1-t22 200.3.1.2/32      192.168.7.133/32
016 1:11 008 *   p wan16      cisco-t221 200.4.103.2/32    192.168.7.133/32
017 1:11 009 *   p wan17      m-e1-t2211 200.4.4.2/32      192.168.7.133/32
018 1:11 010 *   p wan18      m-e1-t2212 200.4.4.3/32      192.168.7.133/32
019 1:17 000 -   p wan19      m2t81      200.8.1.2/32      192.168.7.133/32
020 1:17 000 -   p wan20      m41        200.4.1.2/32      200.6.1.2/32
021 1:16 001 *   p wan21      p1321n<>p1 0.0.0.0/32        0.0.0.0/32
[More? <ret>=next entry, <sp>=next page, <^C>=abort]
```

The output of the `ifmgr` command includes the following fields:

Field	Indicates
`bif`	Bundle interface number. There is one interface number per bundle, including Multilink Protocol Plus™ (MP+) connections. This number is the global interface-table number.
`slot`	Shelf and slot the interface is assigned to.
`sif`	Slot interface.
`u`	Whether the interface is enabled (*) or disabled (-).
`m`	The interface is part of an Multilink Protocol (MP) bundle.
`p`	Whether the interface is permanent. A `P` indicates a permanent interface. A hyphen (-) or a blank indicates that the interface is not permanent. A permanent interface is an interface that is configured in the command-line interface and stored in Stinger NVRAM. All the Ethernet interfaces and the interfaces based on `connection` profiles are permanent. Transient interfaces are those the Stinger unit builds from RADIUS, TACACS, or an `answer` profile. These interfaces have no interface entry when the connection is down.

Field	Indicates
ifname	Interface name.
host-name	Hostname of remote device.
remote-addr	Remote address of device as configured in a connection profile.
local-addr	Local address of device as configured in a connection profile.

To display details about a specific interface name or number, add an interface name or number to the ifmgr -d command. The following sample command displays information about interface 7:

```
admin> ifmgr -d 007
iff             0x82000db0
inUse:          Yes
hostName:
dialoutName:
Authentication Source:  In: local       Out: local
ExternFilters:  No
ExternRoutes @  0
miscInfo @      0
DLCI routeId:   0
rtIf:   0:00:0
virtual id: 0, virtual next @ -1, virtual main @ -1
minor device:   0
device status:  0x20c4
output func:    0x8013ea98
input func:     0x804d27a4
mtu:            65535
ip_addr:        0.0.0.0
dstip_addr:     0.0.0.0
netmask:        255.255.255.255
net:            0.0.0.0
subnet:         0.0.0.0
bcast:          255.255.255.255
nbcast:         255.255.255.255
directed-bcast:         yes
management only:        no
macaddr:        000000000000
inp_qcnt:       0
out_qcnt:       0
nexthop:        0.0.0.0
proxy_arp_mode: 0
proxy_arp_head: 0
No associated connection profile
SNMP ifType:    24
```

The icmp-reply-directed-bcast parameter in the ip-global profile specifies whether the Stinger unit responds to directed-broadcast ICMP echo requests. If this parameter is set to no, the system does not respond to any directed-broadcast ICMP requests. The setting of this parameter is shown in the Directed-Bcast field in the ifmgr output.

Stinger Log Messages

B

The Stinger unit logs fatal and warning error messages to the fatal error log. If the system crashes before creating a log entry, it prints a stack trace to the console serial port. System-status messages, however, go to the Syslog host (if enabled) and the Status log.

Fatal and warning error messages

Each time the system reboots, it logs a fatal error message to the fatal error log. The fatal error log also notes warnings, which indicate situations that did not cause the system to reset. Development engineers use warnings for troubleshooting purposes. When a warning occurs, the system has detected an error condition and has recovered from it. Available flash space limits the number of entries in the fatal error log, and entries rotate on a first-in, first-out (FIFO) basis. to clear the log, use the `clr-history` command.

Reviewing the fatal error log

The system fatal error log contains messages related to Stinger unit operations.

To view the log of fatal errors, use the `fatal-history` command. For example:

```
admin> fatal-history
SYSTEM IS UP:  Index: 100 Revision:9.3-170 first-controller (stngrcm2)
        Date: 04/30/2002.       Time: 12:09:55

PRIMARY SELECTED:Index: 98 Revision:9.3-170 first-controller (stngrcm2)

        Date: 04/30/2002.       Time: 12:10:24

OPERATOR RESET:Index:  99 Revision:9.3-170 first-controller (stngrcm2)
```

```
Date: 04/30/2002.       Time: 14:53:02
Reset from 135.140.144.124, user profile admin.
```

Clearing the fatal error log

Each entry shows the system software version, the slot on which the error occurred, and the date and time at which the error occurred. To clear the log, enter the `clr-history` command:

```
admin> clr-history
```

Fatal and warning messages have the format shown in the following example:

```
Warning:  Index:   171  Revision: 8.0.0  Shelf 1 (stngrcmb)
Date: 06/14/1999.       Time: 16:03:33
Location: 81026460 81069380 81024b38 81024af4 00000000 00000000
```

The first line indicates the type of error (fatal or warning), the index number of the error, the software revision number, the shelf and slot on which the error occurred, and the software load. The fatal log from older software versions display shelf 0.

The second line shows the date and time of the error.

The third line displays the top six program counter addresses from the execution stack active at the time of the crash.

Definitions of fatal errors

Following are definitions, by index number, of the fatal errors that the Stinger unit can report. If you experience a fatal error, contact Lucent OnLine Customer Support at `http://www.lucent.com/support`.

Index	Definition
1	Assert invoked during program execution An Assert has been placed in the code. This problem can be either hardware related or software related.
2	Out of memory during memory allocation This is an out-of-memory condition, sometimes termed a memory leak.
3	Bad profile (T1 DSL related)
4	Switch type bad
5	LIF error
6	LCD error
7	ISAC (BRI) timeout BRI physical layer timeout.
8	Processor exception A processor-exception error caused the reset.
9	Invalid task switch (EXEC)

Index	Definition
10	No mail descriptor (EXEC) This reset occurs if the Stinger tries to allocate a mail message when there are none left. The cause is usually a memory leak.
11	No mail buffer memory (EXEC)
12	No task to run (EXEC)
13	No timer memory (EXEC)
14	No timer pool (EXEC)
15	Wait called while in critical section (EXEC)
16	DSP not responding
17	DSP protocol error
18	DSP internal error
19	DSP loss of sync
20	DSP unused
21	DDD not responding
22	DDD protocol error
23	X25 buffer error
24	X25 init error
25	X25 stack error
27	Memory allocation of zero length
28	Memory allocation of negative length
29	Task infinite loop The reset was the result of a software loop.
30	Too large memory copy
31	Magic sequence missing (MEMCPY)
32	Wrong magic sequence (MEMCPY)
33	Bad start address (MEMCPY)
34	IDEC timeout
35	EXEC restricted
36	Stack overflow
37	DRAM card error Indicates that a DRAM card of unknown size is inserted in the DRAM slot or that the DRAM card failed POST. Applies to the Pipeline® 220 only.

Index	Definition
39	No priority 2 task This error occurs if the Stinger has not run a priority 2 task in the last minute. Tasks in the Stinger are assigned priorities. Because the main routing task runs at priority 2, this error means that Stinger operation has been suspended for 1 minute.
40	Protection fault
41	Memory shortage
60	SNMP-related error
60	SNMP-related error
60	SNMP-related error
99	Operator reset This reset is logged immediately before the Stinger goes down. Instead of a standard stack backtrace, the message includes the active security-profile index. 0 (zero) indicates an unknown security profile. On the Stinger, the Default profile is number 1, and the Full Access profile is number 9.
100	System up As a complement to entry 99, this entry is logged as the Stinger is coming up. For a normal, manual reset, you normally see a fatal error 99 followed by a fatal error 100.

Definitions of warning messages

Warnings are not the results of reset conditions. Most are detected problems from which the Stinger unit typically recovers fully. Following are the definitions, by index number, of the warnings the Stinger unit can report. Warning messages, by themselves, are not necessarily cause for concern. They are used by development engineers to determine the cause of fatal errors.

Contact Lucent OnLine Customer Support at `http://www.lucent.com/support` if warning messages are accompanied by fatal errors.

Index	Definition
101	Buffer already in use
102	Buffer belongs to wrong pool
103	Buffer belongs to wrong heap
104	Buffer not previously allocated This warning can be logged under different conditions. For example, double freeing of memory and low-memory conditions can both generate a warning 104.
105	Buffer bad memory allocation

Index	Definition
106	Buffer belongs to bogus pool
107	Buffer belongs to bogus heap Memory management code (or other modules) detected that the buffer header of what should have been a free buffer was corrupted by the previous overwrite.
108	Buffer negative length memory allocation A negative length request was made to the memory allocation code.
109	Buffer zero length memory allocation This warning is similar to Warning 108, except that a zero length request is made to the memory allocation code.
110	Error in buffer boundary
111	Error buffer too big Indicates that a software routine has tried to allocate a block of memory greater than 64Kbytes.
112	Error buffer null
113	Error buffer segment count zero
114	Error buffer trailer magic
115	Error in buffer trailer
116	Error in buffer trailer length
117	Error in buffer trailer user magic
118	Error buffer write after free
119	Error buffer not in use
120	Error buffer magic in memory copy
121	Error next buffer magic in memory copy
130	PPP async buffer in use Indicates a PPP error.
131	Error with PPP
135	Error with WAN data or WAN sessions
136	Error with WAN data or WAN sessions
140	Error no timers
145	LCD memory allocation failure Indicates that a memory-copy routine was called, but the source buffer was much larger than expected.
146	Invalid state
150	Error memory copy too large
151	Error memory copy magic missing

Index	Definition
152	Error memory copy wrong magic
153	Error memory copy bad start address
154	WAN buffer leak Indicates an error in the WAN drivers.
160	Error in terminal-server state Indicates an error in the WAN drivers.
161	Error in terminal server semaphore
165	Error in Telnet free driver
170	Stac timeout Indicates a hardware error in the Stac compression chip.
171	Stac data not owned Error in the Stac compression chip.
175	EXEC failure Indicates that there is insufficient memory to start a new task.
176	EXEC restricted
177	EXEC no mailbox
178	EXEC no resources
179	Unexpected error
181	Channel display stuck
182	New call without disconnect request Indicates that a Disconnect message to the central office (CO) was not sent. The problem can be caused by conditions on the Stinger or at the CO. When the Stinger encounters the condition, it assumes the CO is correct, and answers the call.
183	New call without disconnect response
184	Disconnect request dropped
185	Spyder buffer error
186	Spyder descriptor error
190	TCP send buffer too big
191	TCP sequence gap
192	TCP too much data
193	TCP write attempt too large
194	TCP options bad
195	Modem message parsing failed
301	TACACS+ pointer inconsistency

Index	Definition
302	TACACS+ index inconsistency
303	TACACS+ TCP inconsistency
304	TACACS+ TCP out-of-range socket
305	TACACS+ socket mismatch
306	TACACS+ unexpected authentication state
381	Error in filter list
382	Error no count in filter list
383	Error mismatch count filter list
550	No Ethernet transmit buffer
1001	Waiting for Ethernet controller
1002	Ethernet ACK command failed
1003	Ethernet reset invoked
1006	Ethernet controller unavailable (wait fail)
1010	Bad Ethernet transmit interrupt
1011	Ethernet transmit not completed
1012	No Ethernet transmit buffer

Fatal crash information on the console

If the system crashes without being able to write to the fatal error log, it prints a stack trace to the console serial port at the bit rate defined in the Serial profile. The trace reports the following information:

`FE:` *N*`, Load:` *loadname*`, Version:` *version*
`Stack trace: 0x`*addr-0* `0x`*addr-1* `0x`*addr-2* `0x`*addr-3* `0x`*addr-4* `0x`*addr-5*

The first line indicates the number of the error and the software revision number.

The second line displays the top six program counter addresses from the execution stack active at the time of the crash.

Syslog messages

Syslog offloads to a host computer known as the Syslog host. The `host` parameter in the `log` profile specifies the Syslog host, which saves the system status messages in a log file.

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

The Stinger unit can report the following session data about various errors logged via Syslog:

Data	Description
`[shelf/slot/line/channel]`	Physical channel identifier.
`[MBID xxx]`	Session identifier. For a given session identifier, multiple physical channel identifiers are possible.
`[name]`	Authenticated name.
`[ calling -> called ]`	Calling number or the called number, or both.
`Progress code`	Lucent-specific code indicating the progress of the call. (For a list of progress codes, see the *Stinger Reference*.)
`Disconnect code`	Lucent-specific code indicating the reason the call was disconnected. (For a list of disconnect codes, see the *Stinger Reference*.)

Accounting records are kept until they are acknowledged by the accounting server. Up to 100 unacknowledged records are stored in the backoff queue. If the unit never receives an acknowledgment to an accounting request, it will eventually run out of memory. In order to keep this situation from the occurring, the unit deletes the accounting records and displays this error message in the syslog file:

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

This error generally occurs for one of the following reasons:

- You enabled RADIUS accounting on the Stinger unit, but not on the RADIUS server.
- The Acct-Port or Acct-Key are incorrect. The Acct-Key must match the value assigned in the RADIUS clients file or the TACACS+ configuration file.
- You are using a Lucent RADIUS server instead of an Ascend RADIUS server.

PCMCIA flash card error messages

When a `load`, `format`, or `dircode` command fails, the Stinger unit logs the messages described in this section.

`load` command messages

Table B-1 lists the error messages that might appear if the system terminates while in the process of loading a tar file.

Table B-1. Load command error messages for loading a tar file

Error message	Description
load aborted: not a tar image	The image you are trying to load is not in tar format.

Table B-1. Load command error messages for loading a tar file (Continued)

Error message	Description
load aborted: a tar image, inconsistent with the specified load-type.	The image header not does not match the load type.
load aborted: invalid/unknown image header.	The image header is missing or corrupt.
load aborted: mismatched image for the specified load-type.	The type checking process discovered inconsistencies between the load type and the image header.
load aborted: invalid image, unsupported by load tar command.	The tar image you are trying to load has been corrupted or is in an unsupported format.

The following warning message does not terminate the load operation, but indicates that you are not loading the most recent software version:

```
load: warning: old image header version detected, load continued...
```

Table B-2 lists the error messages that might appear when you are using the `load` command to upload an image to a PCMCIA flash card on a Stinger unit.

Table B-2. Load command error messages for uploading to a PCMCIA flash card

Error message	Description
`load: error: flash card write failed: card full`	The flash card currently has no space available to load software.
`load: error: specified flash card not present`	No flash card is detected in the specified slot (1 or 2).
`load: error: specified flash card not formatted`	You must enter a `format` command to format the flash card before loading the software.
`load: error: specified flash card has obsolete format`	The flash card was formatted for an older version of the system. You must reformat the card to use it with the current release.
`load: error: specified flash card is write-protected`	The flash card's write-protect switch is set.
`load: error: specified flash image is currently in use`	A control module in the LOAD state is currently accessing the flash card.

`format` command messages

Table B-3 lists the error messages might appear when you are using the `format` command.

Table B-3. Format command error messages

Error message	Description
`error: flash card` *N* `is not present`	No flash card is detected in the specified slot (1 or 2).
`error: flash card` *N* `is unavailable`	The flash card in the specified slot is already being formatted, is just coming up, or is in an error condition.
`error: flash card` *N* `is write-protected`	The write-protect switch is set on the card in the specified slot (1 or 2).
`error: flash card` *N* `is currently in use`	One or more images on the flash card are being read by a module in the LOAD state or are being written as part of a code download.

`dircode` command messages

Table B-4 lists the error messages might appear when you are using the `dircode` command.

Table B-4. Dircode command error messages

Error message	Description
`Card` *N* `is not formatted for use with this system`	The flash card is blank, corrupted, or formatted for another environment, such as DOS. To use this card, you must issue a `format` command first.
`Card` *N* `is temporarily unavailable`	The flash card is currently coming up or is being formatted.
`Card` *N* `is unavailable`	The flash card experienced an error and is inaccessible. Verify that the card is inserted properly.

Table B-4. Dircode command error messages (Continued)

Error message	Description
`Card N uses a format which is no longer supported`	The flash card was formatted for an older version of the operating system. You must reformat the card to use it with the current release.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W