



Stinger[®]

Reference

Copyright © 2000-2004 Lucent Technologies Inc. All rights reserved.

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

Notice

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

European Community (EC) RTTE compliance

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

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

Safety, compliance, and warranty Information

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

Security statement

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

Trademarks

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

Ordering Information

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

How to comment

To comment on this information product, go to the Online Comment Form (<http://www.lucent-info.com/comments/enus/>) or email your comments to the Comments Hotline (comments@lucent.com).

Customer Service

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

Finding information and software

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

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

Obtaining technical assistance

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

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

Obtaining assistance through email or the Internet

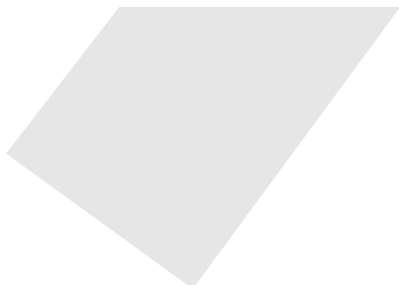
If your services agreement allows, you can communicate directly with a technical engineer through Email Technical Support or a Live Chat. Select one of these sites when you log in to <http://www.lucent.com/support>.

Calling the technical assistance center (TAC)

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

Alternatively, call 1-866-LUCENT8 (1-866-582-3688) from any location in North America for a menu of Lucent services. Or call +1 510-747-2000 for an operator. You must have an active services agreement or contract.

Contents



	Customer Service	iii
	About This Reference	vii
	What is in this reference	vii
	What you should know	vii
	Documentation conventions	vii
	Stinger documentation set	viii
Chapter 1	Stinger Command Reference	1-1
	A	1-3
	B	1-29
	C	1-30
	D	1-37
	E	1-48
	F	1-49
	G	1-61
	H	1-71
	I	1-74
	L	1-89
	M	1-103
	N	1-105
	O	1-116
	P	1-138
	Q	1-162
	R	1-162
	S	1-171
	T	1-192
	U	1-201
	V	1-205
	W	1-208
Chapter 2	Stinger Profile Reference	2-1
	A	2-2
	B	2-18
	C	2-22
	D	2-31
	E	2-37
	F	2-40
	G	2-45

H.....	2-46
I.....	2-48
L.....	2-62
M.....	2-72
N.....	2-76
O.....	2-78
P.....	2-84
Q.....	2-98
R.....	2-100
S.....	2-106
T.....	2-117
U.....	2-129
V.....	2-131
W.....	2-134
X.....	2-135

Chapter 3 Stinger Parameter Reference 3-1

Numeric.....	3-2
A.....	3-5
B.....	3-76
C.....	3-91
D.....	3-133
E.....	3-165
F.....	3-179
G.....	3-203
H.....	3-210
I.....	3-221
j.....	3-249
K.....	3-249
L.....	3-250
M.....	3-281
N.....	3-319
O.....	3-344
P.....	3-358
Q.....	3-393
R.....	3-396
S.....	3-430
T.....	3-492
U.....	3-533
V.....	3-547
W.....	3-561
X.....	3-565
Y.....	3-566

Chapter 4 Progress and Disconnect Codes 4-1

Progress codes	4-1
Disconnect codes	4-3

About This Reference

What is in this reference

This manual provides an alphabetic reference to all the Stinger profiles, parameters, and commands, and details the settings and options you can specify.



Note This manual describes the full set of features for Stinger units running the current True Access™ Operating System (TAOS) software version. Some features might not be available with earlier versions or specialty loads of the software.



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

What you should know

This reference is intended for the person who configures and maintains a Stinger unit. To use it effectively, you must have a basic understanding of Stinger security and configuration and be familiar with authentication servers and networking concepts.

Documentation conventions

Following are 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 can appear on your computer’s screen.
Boldface monospace text	Represents characters that you enter exactly as shown (unless the characters are also in <i>italics</i> —see <i>Italics</i> , following). If you can enter the characters but are not specifically instructed to, they do not appear in boldface.
<i>Italics</i>	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.

Convention	Meaning
[]	Indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in boldface.
	Separates command choices that are mutually exclusive.
>	Separates levels of profiles, subprofiles, and parameters in a hierarchical menu when the path to a menu item is referred to in text.
:	Separates levels of profiles, subprofiles, and parameters in a pathname displayed in the command-line interface or referred to in text.
Key1+Key2	Represents a combination keystroke. To enter a combination keystroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl+H means hold down the Control key and press the H key.)
Press Enter	Means press the Enter, or Return, key or its equivalent on your computer.
Note:	Introduces important additional information.
 Caution:	Warns that a failure to follow the recommended procedure can result in loss of data or damage to equipment.
 Warning:	Warns that a failure to take appropriate safety precautions can result in physical injury.

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 unit 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 2684 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* (this manual). An alphabetic reference to Stinger profiles, parameters, and commands.
 - *TAOS Glossary*. Defines terms used in documentation for Stinger units.

Stinger Command Reference

1

A.....	1-3
B.....	1-29
C.....	1-30
D.....	1-37
E.....	1-48
F.....	1-49
G.....	1-61
H.....	1-71
I.....	1-74
L.....	1-89
M.....	1-103
N.....	1-105
O.....	1-116
P.....	1-138
Q.....	1-162
R.....	1-162
S.....	1-171
T.....	1-192
U.....	1-201
V.....	1-205
W.....	1-208

The information contained here is designed for quick reference. All commands are listed alphabetically.

?

Description Displays a list of all available commands, or help text about a specific command. A list of all available commands also shows the permission level required for the use of each command.

Permission level user

Usage ? [-a] | [command-name]

Command element	Description
-a	List all commands. (Without this option, the list includes only commands authorized by the current user profile.)
command-name	Display information about the specified command.

Example To display a list of commands authorized for your current login:

```
admin> ?
?                               ( user )
alarm                           ( system )
arptable                        ( system )
atmInternalLines                ( system )
atmsig                          ( system )
atmtrunkreset                   ( diagnostic )
AtmTrunks                       ( system )
atmvccstat                     ( system )
atmvcl                          ( system )
atmvcx                         ( system )
atmvpl                          ( system )
atmvpx                         ( system )
auth                            ( user )
briChannels                     ( system )
cat                             ( system )
clear                           ( user )
cleval                          ( system )
clock-source                    ( diagnostic )
[More? <ret>=next entry, <sp>=next page, <^C>=abort]
```

To display help text about a command:

```
admin> ? dir
dir                               list all profile types
dir profile-type                 list all profiles of the specified type
dir profile-type profile-index  list the specified profile instance
```

Dependencies The current security level is set by the current user profile and determines which commands are displayed in response to the ? command. If the current user profile does not have sufficient privileges to execute a command, that command is not displayed unless you include the -a option. By default, commands that go with the current user security level are always displayed. For details, see “auth” on page 1-28.

See Also help, auth

A

adslmibdisplay

Description Display ADSL statistics stored in MIB variables.

Permission level system

Usage adslmibdisplay option port interval-offset

Command element	Description
option	Action that the system takes. Specify one of the following values: ■ t—Display control module time. ■ a—Display physical entry. ■ b—Display channel entry. ■ c—Display performance data interval totals. ■ d—Display channel performance interval totals. ■ p—Display performance data entry. ■ q—Display channel performance entry. ■ i—Display performance data interval. You must also specify an interval-offset value. ■ j—Display channel performance interval. You must also specify an interval-offset value. ■ m—Display monitor parameters. ■ z—Display various variables. ■ f—Display initialization failure information.
port	ADSL port number. You must always specify a port number.
interval-offset	Offset from the current 15-minute interval, backwards in time. You must specify an interval-offset value when you use the i and j options. Valid values are from 1 through 96. A value of 1 specifies the last valid complete 15-minute interval. An interval-offset of 2 specifies the next to last, and forth. A value of 0 specifies the current 15-minute interval and returns an error message because this interval has not completed.

Example Displaying the current time

The `adslmibdisplay t port` command displays the current time retrieved from the active control module. For example:

```
admin> adslmibdisplay t 1
Date: 06/04/2004      Time: 21:06:56
```

Example Displaying ADSL physical entries

The `adslmibdisplay a port` command displays basic ATU-C and ATU-R information. For example:

```
admin> adslmibdisplay a 1

<<< ATU-C Physical Entry >>>
    SerialNum: STGR-LIM-GSA-72
    VendorID: 000000000000000A
    Version: GO-C.12.3.2
    Noise Margin: 130
    Power Attenuation: 20
    Status: 1
    Tx Power: 80
    Attainable Rate: 21604000

<<< ATU-R Physical Entry >>>
    SerialNum:
    VendorID: FFB54753504E0007
    Version:
    Noise Margin: 50
    Power Attenuation: 50
    Status: 1
    Tx Power: 0
    Attainable Rate: 1164000
```

Example Displaying channel entries

The `adslmibdisplay b port` command displays ATU-C and ATU-R train-up data. For example:

```
admin> adslmibdisplay b 1

<<< ATU-C Channel Entry >>>
    InterleaveDelay: 16
    CurrTxRate: 20297000
    PrevTxRate: 0
    CrcBlkLength: 43131

<<< ATU-R Channel Entry >>>
    InterleaveDelay: 16
    CurrTxRate: 1018300
    PrevTxRate: 0
    CrcBlkLength: 2163
```

Example Displaying interval statistics for disruption of service events

For example:

```
admin> adslmibdisplay c 1
Lofs: 0
    Loss: 0
    Lols: 0
    Lprs: 0
    ESS: 0
    Inits: 1
    Num of Valid Intervals: 13
```

Example Displaying interval totals for ADSL block counts

The adslmibdisplay d port command displays ADSL block statistics. For example:

```
admin> adslmibdisplay d 1
      RxBlks: 617612
      TxBlks: 638548
      CorrBlks: 57
      UncorrBlks: 0
      Num of Valid Intervals: 13
```

Example Displaying disruption of service statistics

The adslmibdisplay p port command displays disruption of service statistics for the current 15-minute interval, current one-day interval, and previous one-day interval. For example:

```
admin> adslmibdisplay p 1
<<< ATU-C Performance Data Entry >>>
      Lofs: 0
      Loss: 0
      Lols: 0
      Lprs: 0
      ESs: 0
      Inits: 1
      ValidIntervals: 13
      InvalidIntervals: 0
      Curr15MinTimeElapsed: 897 sec
      Curr15MinLofs: 0 sec
      Curr15MinLoss: 0 sec
      Curr15MinLols: 0 sec
      Curr15MinLprs: 0 sec
      Curr15MinESs: 0 sec
      Curr15MinInits: 0
      Curr1DayTimeElapsed: 12597 sec
      Curr1DayLofs: 0 sec
      Curr1DayLoss: 0 sec
      Curr1DayLols: 0 sec
      Curr1DayLprs: 0 sec
      Curr1DayESs: 0 sec
      Curr1DayInits: 1
      Prev1DayMoniSecs: 0 sec
      Prev1DayLofs: 0 sec
      Prev1DayLoss: 0 sec
      Prev1DayLols: 0 sec
      Prev1DayLprs: 0 sec
      Prev1DayESs: 0 sec
      Prev1DayInits: 0
<<< ATU-R Performance Data Entry >>>
      Lofs: 0
      Loss: 0
      Lols: 0
      Lprs: 0
      ESs: 0
```

```
        Inits: 0
    ValidIntervals: 13
    InvalidIntervals: 0
Curr15MinTimeElapsed: 897 sec
    Curr15MinLofs: 0 sec
    Curr15MinLoss: 0 sec
    Curr15MinLols: 0 sec
    Curr15MinLprs: 0 sec
    Curr15MinESs: 0 sec
    Curr15MinInits: 0
Curr1DayTimeElapsed: 12597 sec
    Curr1DayLofs: 0 sec
    Curr1DayLoss: 0 sec
    Curr1DayLols: 0 sec
    Curr1DayLprs: 0 sec
    Curr1DayESs: 0 sec
    Curr1DayInits: 0
Prev1DayMoniSecs: 0 sec
    Prev1DayLofs: 0 sec
    Prev1DayLoss: 0 sec
    Prev1DayLols: 0 sec
    Prev1DayLprs: 0 sec
    Prev1DayESs: 0 sec
    Prev1DayInits: 0
```

Example Displaying ADSL block counts

The adslmibdisplay q port command displays ADSL block counts for the current 15-minute interval, current one-day interval, and previous one-day interval. For example:

```
admin> adslmibdisplay q 1
<<< ATU-C Channel Performance Data Entry >>>
        RxBlks: 675786
        TxBlks: 698694
        CorrBlks: 60
        UcorBlks: 0
    ValidIntervals: 14
    InvalidIntervals: 0
Curr15MinTimeElapsed: 154
    Curr15MinRxBlks: 7729
    Curr15MinTxBlks: 7991
    Curr15MinCorrBlks: 0
    Curr15MinUcorBlks: 0
Curr1DayTimeElapsed: 12754
    Curr1DayRxBlks: 675786
    Curr1DayTxBlks: 698694
    Curr1DayCorrBlks: 60
    Curr1DayUcorBlks: 0
Prev1DayMoniSecs: 0
    Prev1DayRxBlks: 0
    Prev1DayTxBlks: 0
    Prev1DayCorrBlks: 0
    Prev1DayUcorBlks: 0
```

<<< ATU-R Channel Performance Data Entry >>>

```
RxBlks: 698694
TxBlks: 675786
CorrBlks: 869
UcorBlks: 0
ValidIntervals: 14
InvalidIntervals: 0
Curr15MinTimeElapsed: 154
Curr15MinRxBlks: 7991
Curr15MinTxBlks: 7729
Curr15MinCorrBlks: 11
Curr15MinUcorBlks: 0
Curr1DayTimeElapsed: 12754
Curr1DayRxBlks: 698694
Curr1DayTxBlks: 675786
Curr1DayCorrBlks: 1015
Curr1DayUcorBlks: 0
Prev1DayMoniSecs: 0
Prev1DayRxBlks: 0
Prev1DayTxBlks: 0
Prev1DayCorrBlks: 0
Prev1DayUcorBlks: 0
```

Example Displaying performance data interval

The `adslmibdisplay i port interval-offset` command displays disruption of service statistics for the specified 15 minute interval. For example:

```
admin> adslmibdisplay i 1 1
```

<<< ATU-C Interval Performance Data Entry >>>

```
Number: 13
Lofs: 0 sec
Loss: 0 sec
Lols: 0 sec
Lprs: 0 sec
ESs: 0 sec
Inits: 0
ValidData: 1
```

<<< ATU-R Interval Performance Data Entry >>>

```
Number: 13
Lofs: 0 sec
Loss: 0 sec
Lols: 0 sec
Lprs: 0 sec
ESs: 0 sec
Inits: 0
ValidData: 1
```

```
admin> adslmibdisplay i 1 2

<<< ATU-C Interval Performance Data Entry >>>
      Number: 12
      Lofs: 0 sec
      Loss: 0 sec
      Lols: 0 sec
      Lprs: 0 sec
      ESs: 0 sec
      Inits: 0
      ValidData: 1

<<< ATU-R Interval Performance Data Entry >>>
      Number: 12
      Lofs: 0 sec
      Loss: 0 sec
      Lols: 0 sec
      Lprs: 0 sec
      ESs: 0 sec
      Inits: 0
      ValidData: 1
```

Example Displaying channel performance intervals

The `adslmibdisplay j port interval-offset` command displays channel performance (ADSL block statistics) for the specified interval.

For example, the following command shows ADSL block statistics for the last completed 15-minute interval:

```
admin> adslmibdisplay j 1 1

<<< ATU-C Interval Channel Performance Data Entry >>>
      Number: 14
      recvBlks: 49560
      txBlks: 51240
      corrBlks: 3
      uncorrBlks: 0
      ValidData: 1

<<< ATU-R Interval Channel Performance Data Entry >>>
      Number: 14
      recvBlks: 51240
      txBlks: 49560
      corrBlks: 63
      uncorrBlks: 0
      ValidData: 1
```

The following sample command shows ADSL block statistics for the second to last completed 15-minute interval:

```
admin> adslmibdisplay j 1 2

<<< ATU-C Interval Channel Performance Data Entry >>>
      Number: 13
      recvBlks: 50445
      txBlks: 52155
      corrBlks: 3
      uncorrBlks: 0
      ValidData: 1

<<< ATU-R Interval Channel Performance Data Entry >>>
      Number: 13
      recvBlks: 52155
      txBlks: 50445
      corrBlks: 58
      uncorrBlks: 0
      ValidData: 1
```

Example Displaying monitor parameters

The `adslmibdisplay m port` command displays statistics about the number of disruption of service traps sent. For example:

```
admin> adslmibdisplay m 1
      Monitor Seconds: 13233
      Enable Old Status: 1
      Enable Current Status: 1
      Lofs Trap Sent: 0
      Loss Trap Sent: 0
      Lprs Trap Sent: 0
      Lols Trap Sent: 0
      ESs Trap Sent: 0
      Rate Changed Trap Sent: 0
      Init Fail Trap Sent: 0
```

Example Displaying time and interval information

The `adslmibdisplay z port` command displays time and interval information. For example:

```
admin> adslmibdisplay z 1
      Interval Elapsed Second: 305
      Elapsed Interval Count: 15
      Elapsed Second In A Day: 13805
      Adjusted One Second: 1000
```

Example Displaying initialization failure statistics

The `adslmibdisplay f port` command displays initialization failure counts:

```
admin> adslmibdisplay f 1
      Data Init Fail: 0
      Config Init Fail: 0
      Protocol Init Fail: 0
      No Peer Seconds: 0
```

alarm

Description Enables users to acknowledge, show, and clear alarms.

Permission level system

Usage alarm [-a | -c | -s | -l] address

Command element	Description
-a	Acknowledge alarms.
-c	Clear alarms.
-s	Show alarms. Lists the alarms, the address of the device that has the alarm condition, and the status of the alarm.
-l	List all alarms that are enabled.
address	Location of the alarm, in [shelf slot item] format. If address is unspecified, then the action is for all alarms on the unit. Default values are used for unspecified items

Example To show all alarms, use 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

Example To list all enabled alarms, use the -l option:

```
super> 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

See Also alarm-stat (profile), alarm-state

apsmgr

Description Provides manual controls for protection groups, and displays names, numbers, and modes of the protection groups active in automatic protection switching (APS).

Permission level debug

Usage apsmgr [-a] [-c command aps-cfg-name [channel]
[low-direction]] [-h]

Command element	Description
-a	List all protection groups.
-c	Enter a manual switch command.
-h	Display help text for this command.
command	Specify one of the following: ■ lop—(Lockout of protection). Prevents a working channel from being switched to the protection channel. ■ low—(Lockout of working). Prevents a protection channel from being switched to the working channel. Similar to the lop command, but for the working channel. ■ clow—(Clear lockout of working). Clears the low command for the assigned line. ■ fsw—(Forced switch of working to protection). Switches traffic currently on the working channel to the protection channel. ■ fsp—(Force switch of protection to working). Switches the switched traffic from the protection channel back to the working channel. ■ msw—(Manual switch of protection to working). A low-priority version of the fsw command. ■ msp—(Manual switch of working to Protection). A low-priority version of the fsp command. ■ exer—(EXERcise). Tests the signaling protocol. ■ clear—Clears the following commands: lop, fsw, fsp, msw, msp, exer.
aps-cfg-name	Specifies the name of the aps-config profile—for example, pgl.
channel	Specifies the channel that the command addresses—for example, 1:17:1.

Command element	Description

low-direction	Specifies the direction of the working channel to be locked out by the low command. Valid values are - low-none—The working channel is not locked out. - low-recv—The working channel is locked out in the receive direction only. - low-send—The working channel is locked out in the send direction only. - low-both—The working channel is locked out in both the send and receive directions.

Example The following example uses the -a option to display all protected groups:

```
admin> apsmgr -a
```

Name	PG	Work	Prot	RMode	DMode	State
pg1	255	0:0:0	1:18:2	Rever	Uni	Up

Field	Description

Name	Specifies the name of the protection group, and of the aps-config profile.
PG	Specifies the number of the protection group.
Work	Specifies the address of the working channel.
Prot	Specifies the address of the protection (backup) channel.
RMode	Specifies whether channel operation is revertive (Rever) or nonrevertive (Non-Rev).
DMode	Specifies whether channel directional mode is unidirectional (uni) or bidirectional (bid).
State	Up indicates the protection group is activated and has a valid protection group index; otherwise, Down is displayed.

The following example uses the -c option with the clear command:

```
admin> apsmgr -c clear pg1 1:18:2 none
```

arptable

Description Displays or modifies the Stinger Address Resolution Protocol (ARP) table. Each entry in the ARP table associates a known IP address with a physical address. For remote IP addresses, the Stinger unit can use the ARP table to respond with its own media access control (MAC) address to ARP requests.

Permission level system

Usage arptable [-a IP_address MAC_address] | [-d IP_address] | [-f]

Command element	Description
-a IP address MAC_address	Add an ARP table entry for the device with the specified hostname and MAC address.
-d IP address	Delete the ARP table entry for the device at the specified hostname.
-f	Clear the ARP table.

Example To display the ARP table:

```
admin> arptable
```

IP Address	MAC Address	Type	IF	Retries/Pkts/RefCnt	Timestamp
10.103.0.2	00:C0:7B:7A:AC:54	DYN	0	0/0/552	22760
10.103.0.220	00:C0:7B:71:83:02	DYN	0	0/0/2791	22760
10.103.0.1	08:00:20:7B:24:27	DYN	0	0/0/4296	22811
10.103.0.8	00:00:0C:05:B3:A2	DYN	0	0/0/6493	23058
10.103.0.7	00:00:0C:76:58:4E	DYN	0	0/0/6572	23233
10.103.0.49	00:C0:80:89:19:95	DYN	0	0/0/397	23208

The ARP table displays the following information:

Field	Description
IP Address	Address contained in ARP requests.
MAC Address	MAC address of the host.
Type	How the address is learned, dynamically (DYN) or by specification of a static route (STAT).
IF	Interface on which the Stinger unit receives the ARP request.
Retries	Number of retries needed to refresh the entry after it times out.
Pkts	Number of packets sent out to refresh the entry after it times out.
RefCnt	Number of times the Stinger unit consults the entry.
Time Stamp	Number of seconds since the system has started up. The Stinger unit updates this field every time an ARP entry is refreshed.

Example To add an ARP table entry for a device with the physical address 00A024A61535 at IP address 10.9.8.20:

```
admin> arptable -a 10.9.8.20 00A024A61535
```

See Also nslookup

atmcacstat

Description Displays statistics about connection admission control (CAC) bandwidth allocation.

Permission level system

Usage atmcacstat - s | b | p | a | r | c service

Command element	Description
-s	Display CAC entry summary.
-b shelf slot	Display CAC bandwidth allocation for specified slot and shelf.
-p	Display bandwidth allocation for trunk ports.
-a	Display all bandwidth allocation for all active connections.
-c service	Display bandwidth allocation for a specified service category. Specify one of the following values with the -c option: ■ 0—Constant bit rate (CBR) ■ 1—Real-time variable bit rate (RTVBR) ■ 2—Non-real-time variable bit rate (NRTVBR) ■ 3—Unspecified bit rate (UBR)

Example To display bandwidth allocation by slot, use the -b option as follows:

```
admin> atmcacstat -b

BANDWIDTH INFORMATION FOR SLOT 1
UP STREAM
  Total B/W Kbits/sec      : 70000
  Guaranteed B/W Kbits/sec : 42500
  Allocated Guaranteed B/W : 40000
  Available Guaranteed B/W  : 2500
DN STREAM
  Total B/W Kbits/sec      : 148598
  Guaranteed B/W Kbits/sec : 148598
  Allocated Guaranteed B/W : 40000
  Available Guaranteed B/W  : 108598
BANDWIDTH INFORMATION FOR SLOT 2
UP STREAM
  Total B/W Kbits/sec      : 70000
  Guaranteed B/W Kbits/sec : 42500
  Allocated Guaranteed B/W : 0
  Available Guaranteed B/W  : 42500
DN STREAM
  Total B/W Kbits/sec      : 148598
  Guaranteed B/W Kbits/sec : 148598
  Allocated Guaranteed B/W : 0
  Available Guaranteed B/W  : 148598
```

Example To display the CAC bandwidth allocation for the trunk module ports, use the -p option:

```
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      148598          148598  0              148598
DN      148598          148598  0              148598

PORT {1 17 2} (oc3-atm-trunk-daughter-card) (ACTIVE) (PRIMARY)
Stream  Total BW      Gtd BW  Gtd Allocated  Gtd Available
UP      148598          148598  0              148598
DN      148598          148598  0              14859840644

PORT {1 18 1} (ds3-atm-trunk-daughter-card) (ACTIVE) (PRIMARY)
Stream  Total BW      Gtd BW  Gtd Allocated  Gtd Available
UP      40644          40644  0              40644
DN      40644          40644  0              40644

PORT {1 18 2} (ds3-atm-trunk-daughter-card) (ACTIVE) (PRIMARY)
Stream  Total BW      Gtd BW  Gtd Allocated  Gtd Available
UP      40644          40644  40000          644
DN      40644          40644  40000          644
```

Example To display bandwidth allocation for the CBR service category, use the -c option with the 0 value:

```
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

atmconnectionfailures

Description atmConnectionFailures is a system command for displaying information about asynchronous transfer mode (ATM) connection failures.

Permission level system

Usage atmConnectionFailures

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

atminternallines

Description Displays statistics for the Asynchronous Transfer Mode (ATM) internal lines.

Permission level system

Usage atminternallines -[a | d | f | u]

Command element	Description
-a	Show all lines.
-d	Show disabled lines.
-f	Show all free lines.
-u	Show in-use lines.

Example To display statistics for all ATM lines:

```
admin> atminternallines -a
```

All ATM Internal lines:

	(dvOp	dvUpSt	dvRq	sAdm	nailg)
{ 1 17 2 }	(Up	Idle	UP	UP	00802)

The data displayed includes the physical address of each line and the following information:

Field	Description
dvOp	The 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	The 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	The 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	The 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. The 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	The dedicated (nailed) group to which the line is assigned.

See Also atmqos, atm-if-config (profile), atm-internal (profile), atm-options

atmqos

Description Displays quality of service (QoS) statistics on Asynchronous Transfer Mode (ATM) connections.

Permission level diagnostic

Usage atmqos -[a|c|d] qos-name

Syntax Element	Description
-a	Show QoS statistics on all ATM connections.
-c qos-name	Show all connections that use the specified atm-qos profile (the QoS Name in the atmqos -a output).
-d qos-name	Display QOS statistics for the specified atm-qos profile (the QoS Name in the atmqos -a output) only.

Example To display QoS statistics on all ATM connections:

```
admin> atmqos -a
```

Td Index	QoS Name	Category	PCR (Cells Per Second)	SCR (Cells Per Second)	MCR (Cells Per Second)
1	default	UBR	0	-	-
2	default-ctl	NRT_VBR	75	75	-
3	default-rcc	NRT_VBR	905	452	-
4	default-ilmi	NRT_VBR	37	37	-
5	pseudo-abr-sig	ABR	471	-	235

Label	Description
Td Index	Traffic descriptor index.
QoS Name	Name assigned to the atm-qos profile.
Category	Quality of service (QoS).
PCR	Peak cell rate in number of cells per second.
SCR	Sustainable cell rate in number of cells per second.
MCR	Minimum cell rate in number of cells per second.

Example Examples using the -c and -d options follow:

```
admin> atmqos -c atmqos416
vc-11-1-0-35
Total Number Of Connections : 1

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
```

See Also atminternallines, atmtrunks, atmvcstat, imagroups, imalines

atmsig

Description Displays signaling statistics for an Asynchronous Transfer Mode (ATM) connection.

Permission level system

Usage atmsig [[-i interface] | [-c interface] | -p | shelf slot port]]

Command element	Description
-i interface	Show ATM signaling statistics by interface.
-p shelf slot port	Show ATM signaling statistics by shelf, slot and port.
-c interface	Clear ATM signaling statistics by interface.

Example To display ATM signaling 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
```

See Also atmtrunks, atmccstat

atmtrunkmgr

Description Indicates the status of connections for Asynchronous Transfer Mode (ATM) trunk modules and their connections.

Permission level system

Usage atmtrunkmgr [-t | -g connection-profile-name nailed-group]

Command element	Description
-t	Toggle 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.
-g connection-profile 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).

Example The following example commands switch debug levels from 1 to 2:

```
admin> atmtrunkmgr -t
current atmtrunkmgr debug level = 1
admin> atmtrunkmgr -t
current atmtrunkmgr debug level = 2
```

The following example queries a connection named ckt with nailed group 801:

```
admin> atmtrunkmgr -g ckt 801
return from atmTrunkDevGetChansByNGAndProf chan= 1.
```

See Also atmtrunkreset, atmtrunks, atmvc1, atmvcx, atmvp1

atmtrunkreset

Description Resets the unit's trunk modules.

Permission level diagnostic

Usage atmtrunkreset [-17|-18]

Command element	Description
No options	Display the options for this command.
-17	Reset trunk module 1.
-18	Reset trunk module 2.

See Also atmtrunks

atmtrunks

Description Indicates the status of the Asynchronous Transfer Mode (ATM) trunk modules on a Stinger unit.

Permission level system

Usage atmtrunks [-a | -c [slot [port]] | -d | -f | -s | -u]

Command element	Description
-a	Show all ATM trunks.
-c [slot [port]]	Reset trunk statistics for OC3-ATM and DS3-ATM trunk modules. ■ When you use the slot option, the unit resets trunk statistics for the specified slot. ■ When you use the port option with the slot option, the unit resets trunk statistics for the specified port. ■ When you do not use any options, the unit resets trunk statistics for all OC3-ATM and DS3-ATM trunk modules.

Command element	Description
-d	Show disabled trunks.
-f	Show all free trunks.
-s	Show trunk port redundancy operations.
-u	Show in-use trunks.

Example To display the status of all ATM trunk modules:

```
admin> atmtrunks -a
All OC3 ATM trunks:
OC3 Lines          m(dvOp  dvUpSt  dvRq    sAdm  nailg)
Line   {    1 17  1  } (Down  Idle    UP      UP    00801)
Line   {    1 17  2  } (Up    Idle    UP      UP    00802)

All DS3 ATM trunks:
DS3 Lines(          dvOp    dvUpSt  dvRq    sAdm  nailg)
Line   {    1 18  1  } (Up    Idle    UP      UP    00851)
Line   {    1 18  2  } (Down  Idle    UP      UP    00852)

All E3 ATM trunks:
E3 Lines            (dvOp    dvUpSt  dvRq    sAdm  nailg)
```

Example To clear trunk statistics for all trunks:

```
admin> atmtrunks -c
Clearing ATM Trunk Statistics for All Trunks
```

Example To clear trunk statistics for a specific slot:

```
admin> atmtrunks -c 17
Clearing ATM Trunk Statistics for Slot 17
```

Example To clear statistics for a specific port on a trunk module:

```
admin> atmtrunks -c 17 1
Clearing ATM Trunk Statistics for Slot 17 port 1
```

See Also atmtrunkmgr, atmvccstat

atmvccstat

Description Displays the ATMVCC status window, which shows active Asynchronous Transfer Mode (ATM) virtual channel connections (VCCs) in the following format:

slot/port/virtual path identifier (VPI)/virtual channel identifier (VCI)

The command also displays the receive (Rx) and transmit (Tx) cell counts for ATM VCCs.

Permission level system

Usage atmvccstat

Example To display the ATMVCC status window:

```
admin> atmvcstat

2 Connections                                x Status
0002 17-1-48                                x Serial number: 10048257
Version: 9.0-126e0
0001 17-1-47                                x
x Rx Pkt:                                16906
x Tx Pkt:                                4488
x   Col:                                5
x
06/14/2024      02:49:15 Up: 0    days,      00:39:00
17/ 2/ 0/      Rx:125      Tx:322
17/ 1/ 0/      Rx:401      Tx:117
17/ 2/ 0/      Rx:54       Tx:32
```

See Also atmtrunks, atmvcx

atmvcl

Description Displays Asynchronous Transfer Mode (ATM) virtual channel links (VCLs).

Permission level system

Usage atmvcl [-c | -a | -sh shelf | -s shelf slot | -p shelf slot port | -d shelf slot port vpi vci]

Command element	Description
-c	Show a count of the different types of calls. The system displays the number of terminating permanent virtual circuits (PVCs), PVC segments without cross-connections (created by SNMP), and PVC segments with cross-connections in a Stinger unit. This option can be used with the -a (default), -s, or -p options.
-a	Show all ATM VCLs.
-sh shelf	Show ATM VCLs by shelf.
-s shelf slot	Show ATM VCLs by slot.
-p shelf slot port	Show ATM VCLs by slot and port.
-d shelf slot port vpi vci	Show detailed ATM VCL info.

Command element	Description
grep argument	Searches for the value argument. See the grep command.

Example To show a count of different types of calls:

```
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
```

Example To show all VCLs:

```
admin> atmvcl -a
Intf Shelf Slot Port Vpi Vci XConnID Kind OStatus
11 1 17 1 0 900 3 pvc up
11 1 17 1 0 902 2 pvc up
11 1 17 1 0 999 6 pvc up
11 1 17 1 0 1000 1 pvc up
11 1 17 1 0 1001 4 pvc up
11 1 17 1 0 1002 5 pvc up
61 1 1 1 0 35 6 pvc up
62 1 1 2 0 35 4 pvc up
63 1 1 3 0 35 5 pvc up
311 2 1 1 0 35 1 pvc up
318 2 1 8 0 35 2 pvc up
319 2 1 9 0 35 3 pvc up

Totals:                Up      Down
PVC XConnect           12        0
PVC Terminate           0        0
PVC Legs Only           0        0
SVC In                  0        0
SVC Out                 0        0
SPVC Initiator          0        0
SPVC Target             0        0
Invalid                  0
```

Example To show all VCLs on remote shelf 2:

```
admin> atmvcl -sh 2
Intf Shelf Slot Port Vpi Vci XConnID Kind OStatus
311 2 1 1 0 35 1 pvc up
318 2 1 8 0 35 2 pvc up
319 2 1 9 0 35 3 pvc up
...
```

Example To show the VCLs on slot 1 of remote shelf 2:

```
admin> atmvcl -s 2 1
Intf Shelf Slot Port Vpi Vci XConnID Kind OStatus
311 2 1 1 0 35 1 pvc up
318 2 1 8 0 35 2 pvc up
319 2 1 9 0 35 3 pvc up
...
```

Example To show the VCLs in VPI 0 and VCI 35 on port 9 of slot 1 on remote shelf 2:

```
admin> atmvcl -d 2 1 9 0 35
PA = { 2 1 9 }, physIF = 283, nextIf = 319
Physical Address = { 2 1 9 }
Interface = 319
VCC Endpoint = no
Vpi = 0
Vci = 35
Oper Status = up
Rx Traffic Descr Index = 1
Tx Traffic Descr Index = 1
Conn Kind = pvc
Cast Type = p2p
Cross Connect ID = 3
```

Example To show only VCLs that include the value 41:

```
admin> atmvcl -a | grep 41
Intf Shelf Slot Port Vpi Vci XConnID Kind OStatus
116 2 6 1 0 41 23 spvcI up
120 2 6 3 0 41 0 pvc down

<grep> Found 2 line(s) matching search criteria

Totals:          Up   Down
PVC              2    5
SVC In           0    0
SVC Out          13    0
SPVC Initiator   13    0
SPVC Target      0    0
Invalid          0
```

See Also atmtrunkreset, atmvcx, atmvp1, atmvpX, grep

atmvcx

Description Displays Asynchronous Transfer Mode (ATM) virtual channel cross-connects. A cross-connect receives a cell stream on one interface and transmits it on another.

Permission level system

Usage atmvcx [-a | -sh shelf | -s shelf slot | -p shelf slot port]

Command element	Description
-a	Show all ATM virtual channel cross-connects.
-sh shelf	Show ATM virtual channel cross-connects by shelf.
-s shelf slot	Show ATM virtual channel cross-connects by slot.
-p shelf slot port	Show ATM virtual channel cross-connects by slot and port.

Example To display information about all virtual channel cross-connects on slot 1 of remote shelf 2:

```
admin> atmvcx -s 2 1
```

Profile	Kind	Low							High						
		Intf	Sh	Sl	Port	VPI	VCI	Oper	Intf	Sh	Sl	Port	VPI	VCI	Oper
Permanent VC X-Connects:															
pvc-2-1-1	pvc	11	1	17	1	0	1005	up	311	2	1	1	0	35	up
pvc-2-1-8	pvc	11	1	17	1	0	902	up	318	2	1	8	0	35	up
pvc-2-1-9	pvc	11	1	17	1	0	900	up	319	2	1	9	0	35	up

Field	Indicates
Profile	Name of the profile in which the ATM circuit is configured.
Kind	Call control type.
Intf	ATM interface index.
Sh	Shelf on which a virtual channel link (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.
Sl	Slot on the specified shelf on which a virtual channel link (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.

Field	Indicates
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	Virtual path identifier (VPI) assigned to the VCL.
VCI	Virtual channel identifier (VCI) assigned to the VCL.
OStatus	Current operational status of the cross-connect.

See Also atmtrunkreset, atmvc1, atmvp1, atmvpX

atmvpl

Description Displays statistics about the Asynchronous Transfer Mode (ATM) virtual path links (VPLs).

Permission level system

Usage atmvpl [-a | -sh shelf | -s shelf slot | -p shelf slot port | -d shelf slot port vpi]

Command element	Description
-a	Show all ATM VPLs.
-sh shelf	Show ATM VPLs by shelf.
-s shelf slot	Show ATM VPLs by slot.
-p shelf slot port	Show ATM VPLs by slot and port.
-d shelf slot port vpi	Show detailed ATM VPL info.

Example To display all ATM VPLs:

```
admin> atmvpl -a
Intf  Shelf  Slot  Port  Vpi  XConnID  Kind  OStatus
15    1      18    1     10    1        pvc   up
16    1      18    2     20    1        pvc   up
...
```

Example To display the ATM VPLs in slot 18:

```
admin> atmvpl -s 18
Intf  Shelf  Slot  Port  Vpi  XConnID  Kind  OStatus
15    1      18    1     10    1        pvc   up
16    1      18    2     20    1        pvc   up
...
```


Example To display the ATM VPLs in shelf 2, slot 18 for port 1, VPI 20:

```
admin> atmvpix -d 2 18 1 20
Physical Address = { 2 18 1 }
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
```

See Also atmvc1, atmvcx, atmvpix

atmvpix

Description Displays Asynchronous Transfer Mode (ATM) virtual path cross-connects. A cross-connect receives a cell stream on one interface and transmits it on another.

Usage atmvpix [-a | -sh shelf | -s shelf slot | -p shelf slot port]

Command element	Description
-a	Show all ATM virtual path cross-connects.
-sh shelf	Show ATM virtual path cross-connects by shelf.
-s shelf slot	Show ATM virtual path cross-connects by slot.
-p shelf slot port	Show ATM virtual path cross-connects by slot and port.

Example To display all information about virtual path cross-connects on slot 1 on remote shelf 2:

```
admin> atmvpix -s 2 1
                                     Low                                     High
Profile      Kind Intf/ Sh/Sl/Port/ VPI/Oper Intf/ Sh/Sl/Port/ VPI/Oper
pvc-vp-2-1-5  pvc  11  1 17   1   11 down  255  2 1   5   15 down
```

Field	Indicates
Profile	Name of the profile in which the ATM circuit is configured.
Kind	Call control type.
Intf	ATM interface index.

Field	Indicates
Sh	Shelf on which a virtual channel link (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.
Sl	Slot on the specified shelf on which a virtual channel link (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	Virtual path identifier (VPI) assigned to the VCL.
VCI	Virtual channel identifier (VCI) assigned to the VCL.
OStatus	Current operational status of the cross-connect.

See Also atmvc1, atmvcx, atmvp1

auth

Description Authenticates your current login by applying a specified user profile. Use this command to increase or decrease the permissions of the current login. For information about permission levels in user profiles, see the description of the user profile.

Permission level user

Usage auth user-name

Command element	Description
user-name	Authenticate the specified user profile.

Example To log in as Joe:

```
admin> auth joe
Password:
```

If you supply the proper password for the user profile you have specified, the Stinger unit enables the privileges in that profile and then displays the system prompt again. The user profile can specify its own system prompt, which is a useful way to indicate certain permission levels. For example:

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

If you supply the wrong password at the prompt, the following message appears:

```
Login incorrect
User:
```

Enter the username again to display the Password prompt.

See Also `whoami`, `?`

B

`brichannels`

Description Displays statistics for Basic Rate Interface (BRI) channels.

Permission level `system`

Usage `brichannels [-a | -d | -c | -i]`

Command element	Description
<code>-a</code>	Show all available channels.
<code>-d</code>	Show disabled channels.
<code>-c</code>	Show all possible channels.
<code>-i</code>	Show in-use channels.

Example To display all available BRI channels:

```
admin> brichannels -a
BRI channels available for use:
          (dvOp dvUpSt dvRq sAdm nailg)
```

See Also `ids1-bandwidth`

C

caleashow

Description Displays information about all Communications Assistance for Law Enforcement Act (CALEA) leaf connections and their associated root connections.

Permission level system

Usage caleashow

Example To display information about all CALEA connections:

```
admin> caleashow
Calea Connection  Root Connection  This Side          Other Side
-----
calea1            root1             {18/1 /0 /67 } {18/1 /0 /68 }
calea2            root1             {18/1 /0 /67 } {18/1 /0 /67 }
```

Field	Displays
Calea Connection	Name of the CALEA leaf connection profile.
Root Connection	Name of the root connection profile associated with the CALEA leaf connection.
This Side	Interface, virtual path identifier (VPI), and virtual channel identifier (VCI) specified in the atm-options subprofile of the root connection profile. If this field is empty, the virtual channel connection (VCC) is not being intercepted by the CALEA connection.
Other Side	Interface, virtual path identifier (VPI), and virtual channel identifier (VCI) specified in the atm-connect-options subprofile of the root connection profile. If this field is empty, the VCC is not being intercepted by the CALEA connection.

cat

Description Prints a file residing on a PCMCIA flash memory card to the screen to help you verify the contents of a saved configuration file.

Permission level system

Usage cat [socket [/pathName]]

Command element	Description
socket	The number of the flash card slot—for example, 1.
pathname	The directory and the filename on the flash card. Normally, the file contains a saved configuration.

Example admin> cat 1/config/asavecfg.txt

Dependencies The flash card must formatted.

See Also `ls`, `format`, `mkdir`, `mv`, `rm`, `save`

`changepasswd`

Description The `changepasswd` command enables a user to change their password from the terminal session.

Permission level `user`

Usage `changepasswd`

Dependencies If password validation is enabled for the user's account (the `enforce-password-check` parameter in the user profile is set to yes), the new password must be at least 8 characters long, containing at least two numbers and four alphabetical characters.

`chassisdesc`

Description Displays the name of the platform that is operating.

Permission level `user`

Usage `chassisdesc`

Example To display the platform name:

```
admin> chassisdesc  
Lucent Stinger-10
```

`clear`

Description Clears the command-line interface screen or the terminal session screen. The system prompt appears at the top row of the command-line interface screen, or the top row of the VT100 window used in the terminal session display.

Permission level `user`

Usage `clear [-r]`

Command element	Description
<code>-r</code>	Reset the terminal session's terminal display attributes.

See Also `screen`

`clevall`

Description Shows whether the call logging 30-day evaluation license is granted.

Permission level `system`

Usage cleval

Example admin> cleval

This machine is already licensed for Network Management and it is capable of emitting call logging records

clock-source

Description Displays the current clock-source settings for the system. If a line is specified as the master clock source, it provides the source of timing information for synchronous connections. The clock allows the sending device and the receiving device to determine where one block of data ends and the next begins.

If multiple lines specify that they are eligible to be the clock source, you can assign clock-source priority among multiple lines. In the output of the `clock-source` command, the value 1 signifies the highest priority.

Permission level diagnostic

Usage clock-source

Example The `clock-source` command on the control module shows the master clock's module line number:

```
admin> clock-source
Master line: 1
Source List:
      Source: line 1 Available*      priority: 2
      Source: line 3 Available      priority: 2
```

On the modules, the `clock-source` command uses one-base indexes for the module's lines. For example, to open a session with a DS3-ATM trunk module and display its clock-source settings:

```
admin> open 1 1
ds3-1/2> clock-source
Master line: 1
Source List:
      Source: line 1 Available*      priority: 2
      Source: line 3 Available      priority: 2
```

Following are examples of log messages generated for clock-source transitions:

```
LOG notice, Shelf 1, Controller, Time: 19:44:39--
Master clock source changed to slot-1/8 line 1
LOG notice, Shelf 1, Controller, Time: 10:34:56--
Master clock source changed to local oscillator
```

Dependencies The `clock-source` command lists only currently eligible local clock sources. Sources with Layer 2 up, which are preferred, are marked with an asterisk. In addition, a message is logged whenever the system clock source changes. You must first execute the `open` command to open a session with the module.

See Also `open`, `clock-priority`

clr-history

Description Clears the fatal-error history log.

Permission level system

Usage clr-history [-f]

Command element	Descriptions
-f	Forces the clear operation without requiring verification. Use this option if entering only clr-history does not clear the fatal-history log.

Example To clear the fatal-error history log:

```
admin> clr-history
```

See Also fatal-history

cltactivate

Description Enables a copper loop test (CLT).

Permission level system

Usage cltactivate [-s remote_shelf] [-t timeout] slot port [cltslot
[mode [terminal [loop]]]]

Command element	Description
-s remote_shelf	On hosted Stinger systems, identifies the remote shelf on which to run the copper loop test. The command is entered from the host Stinger unit.
-t timeout	Specify a timeout value in minutes for the copper loop test from 0 through 30, where 0 means no timeout.
slot	Slot number of the LIM containing the copper loop to be tested.
port	Port number of the copper loop to be tested.
cltslot	Slot number of the copper loop test (CLT) module or path selector module (PSM) running the test.
mode	Connection configuration of the copper loop. The default value, <i>bridged</i> , specifies that the copper loop is connected to the test head and the corresponding port of the spare LIM. Specify <i>looking-out</i> to connect the copper loop only to the test head.

Command element	Description

terminal	Connection point of the copper loop. Specify one of the following values: ■ internal-tester-terminal—Copper loop is connected to the internal test head of the CLT module. If you specify no argument, the system takes this default value. ■ external-tester-terminal—Copper loop is connected to the external test terminals of the CLT module or PSM. ■ auxiliary-tester-terminal—Copper loop is connected to the auxiliary test terminals of the CLT module or PSM.
loop	Copper loop number of the T1 or E1 port. This parameter applies only to copper loops connected to T1 or E1 LIMs, and is ignored for all other LIMs. 1—Transmit copper loop. 2—Receive copper loop.



Note For a detailed discussion of this command and all its parameters, see the *Stinger Copper Loop Test (CLT) Module Guide*.

See Also `cltactivate external-loop`, `cltdeactivate`, `cltcmd`

`cltactivate external-loop`

Description Sets a copper loop test (CLT) module to external-loop access mode. The CLT slot is detected automatically and the access mode is set to looking-out.

Permission level system

Usage `cltactivate [ -s remote_shelf ] external-loop`

See Also `cltactivate`, `cltdeactivate`, `cltcmd`

`cltcmd`

Description Runs a copper loop test (CLT).

Permission level system



Note For a detailed discussion of this command and all its parameters, see the *Stinger Copper Loop Test (CLT) Module Guide*.

See Also `cltactivate`

`cltdeactivate`

Description Disables a copper loop test (CLT).

Permission level system

Usage cltdeactivate [-s remote_shelf] [cltSlot]



Note For a detailed discussion of this command and all its parameters, see the *Stinger Copper Loop Test (CLT) Module Guide*.

See Also cltactivate

cltextend

Description Extend the duration of an activated copper loop test.

Permission level system

Usage cltextend [-s shelf]

Command element	Description
-s shelf	Extend the duration of the copper loop test on a specified shelf.

Example Following is an example of the cltextend command:

```
admin> cltextend
LOG notice, Shelf 1, Controller-1, Time: 10:13:36--
    Copper loop access extended at shelf 1
```

Dependencies On hosted systems, when you use the -s shelf argument, you must enter the command from the controller on the host shelf.

cmmodemshowcountries

Description Displays a list of the countries supported by the modem installed in a revision 2 control module.

Permission level system

Usage cmmodemshowcountries

Example To display a list of the countries supported by a modem:

```
admin> cmmodemshowcountries
The country codes supported by this modem are:
0, Japan
9, Australia
a, Austria
f, Belgium
16, Brazil
26, China
31, Denmark
3c, Finland
3d, France
42, Germany
46, Greece
53, India
57, Ireland
```

59, Italy
61, Korea
6c, Malaysia
73, Mexico
7b, Netherlands
82, Norway
8a, Poland
8b, Portugal
9c, Singapore
9f, South Africa
a0, Spain
a5, Sweden
a6, Switzerland
b4, United Kingdom
b5, United States
fd, unknown
fe, Taiwan

`cmmodemshowcurrentcountry`

Description Displays the country code that is currently configured for a modem.

Permission level debug

Usage `cmmodemshowcurrentcountry`

Example To display the country code currently configured for a modem:

```
admin> cmmodemshowcurrentcountry
```

The country code programmed is b5, United States

`connection`

Description Specifies that the upper left portion of the status window displays connection status information. If the status window is not already displayed, this command opens it with the connection status information displayed.

Permission level system

Usage `connection`

Example To open a window with connection status information displayed:

```
admin> connection
```

Press the Escape key to display a prompt below the status window

See Also `clear`, `list`, `log`, `screen`, `status`, `view`

D

date

Description Displays or sets the Stinger system date and time. The date and time are stored in the `timedate` profile.

Permission level `update`

Usage `date`

Example `admin> date`

Wed Mar 7 16:17:41 2001

Dependencies You can set the Stinger system date and time in the `timedate` profile.

See Also `TIMEDATE`

debug

Description Enables or disables diagnostic output.

Permission level `diagnostic`

Usage `debug on | off`

Command element	Description
<code>on</code>	Enables diagnostic output.
<code>off</code>	Disables diagnostic output.

Example To enable diagnostic output:

```
admin> debug on
Diagnostic output enabled
admin> FRMAIN: Setting timer DCE
FRMAIN: time 88121200, mkstatus type 1, seq (026,025)
```

See Also `auth`

degen-tone

Description Stops multiport tone testing on the ports of a line interface module (LIM) in the designated slot of a Stinger unit.

Permission level `system`

Usage `degen-tone shelf slot`

Command element	Description
<code>shelf</code>	Shelf of the LIM whose ports are being tested.

Command element	Description
slot	Number of a slot in a Stinger unit.

Example To stop multiport tone testing on a LIM in shelf 1, slot 5:

```
admin> degen-tone 1 5
```

See Also gen-tone

deisolate

Description Stops galvanic isolation testing on the ports of a line interface module (LIM) in the designated slot of a Stinger unit.

Permission level system

Usage deisolate shelf slot

Command element	Description
shelf	Shelf of the LIM whose ports are being tested.
slot	Number of a slot in a Stinger unit.

Example To stop galvanic isolation testing on a LIM in shelf 1, slot 5:

```
admin> deisolate 1 5
```

See Also isolate

delete

Description Permanently deletes a profile from local storage. Any flash memory space that was used by the profile becomes available to the system.

Permission level update

Usage delete [-f] profile-type [profile-index]

Command element	Description
-f	Delete without prompting for confirmation.
profile-type	Type of profile, as listed by the dir command.
profile-index	The index of the specified profile type. Not all profile types require an index.

Example To delete the connection profile previously created for Tom Lynch:

```
admin> delete conn tlynch
Delete profile CONNECTION /tlynch? [y/n] y
CONNECTION /tlynch deleted
```

See Also get, new, read

device

Description Initiates a state change in a specified device. The device is specified by its interface address. This command is typically used to administratively put the device in an UP or DOWN state.

Permission level diagnostic

Usage device -d|-t|-u|-? interface_address

Command element	Description
-d	Put the specified device in a DOWN state.
-u	Put the specified device in an UP state.
interface_address	Interface address of the device, specified as shelf, slot, item number, and logical item number.

Example To administratively disconnect device 24 in slot 3 on shelf 1:

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

See Also show, slot

dir

Description Lists profiles. With no options, the dir command lists all profile types supported by the Stinger unit. It can also be used to list all profiles of a certain type, or to list file-system information about a specific profile.

Permission level system

Usage dir [profile-type [profile-index]]

Command element	Description
profile-type	List all the profiles of the specified type.
profile-index	Display information about the specified profile.

Example To list all profile types, enter the dir command with no variables:

```
admin> dir
ADMIN-STATE-PERM-IF  SNMP Permanent Interface Admin State
ADMIN-STATE-PHYS-IF  SNMP Physical Interface Admin State
AL-DMT-STAT          Dmt Alcatel adsl line status
```

AL-DMT	Alcatel cell dmt adsl line parameters
ANSWER-DEFAULTS	Answer profile
ATMPVC-STAT	ATM PVC State
ATMVCC-STAT	ATM VCC State
BANDWIDTH-ALLOC	Bandwidth allocation for slots for ATM
BANDWIDTH-STATS	Bandwidth statistics for slots for ATM
BASE	System version and enabled features
CALL-INFO	Active call information
CALL-LOGGING	Call logging
CONNECTION	Connection (WAN) profiles
DEVICE-STATE	Device Operational State
DEVICE-SUMMARY	Device availability summary information
ERROR	Fatal Error log
ETHER-INFO	Ethernet Interfaces Information
ETHERNET	Ethernet Interfaces Configuration
EXT-TSRV	Remote Terminal Server Config Information
EXTERNAL-AUTH	External authentication info
IP-GLOBAL	Global TCP/IP parameters
IP-INTERFACE	IP interfaces
IP-ROUTE	Static IP routes
LOAD-SELECT	Code images to load
LOG	System event logging configuration
SDSL	Sdsl line parameters
SDSL-STAT	Sdsl line status
SERIAL	Serial interfaces
SLOT-INFO	Slot Info profile
SLOT-STATE	Slot Operational State
SLOT-TYPE	Slot Type profile
SNMP	SNMP configuration
SYSTEM	System-wide basic parameters
TERMINAL-SERVER	Terminal server parameters
TIMEDATE	Current system date and time
TRAP	SNMP trap destinations
USER	Administrative user accounts

Example To list all connection profiles, as well as all RADIUS profiles for dedicated (nailed) connections, specify conn as the profile type. For example:

```
admin> dir conn
169 08/31/2002 22:21:07 dallas
195 09/12/2002 10:14:08 chicago
189 11/14/2002 09:34:44 nyc1
177 11/14/2002 11:38:09 nyc2
187 10/22/2002 15:34:53 la
201 10/14/2002 14:29:32 sacto
```

This form of the command is useful for displaying valid profile indexes. The index is in the rightmost field. The listing includes the following information:

- The first field shows the number of bytes that the profile uses.
- The second field shows the date that the profile was last modified.
- The third field shows the time that the profile was last modified.
- The fourth field shows the profile index. If the profile does not have an index, the fourth field contains a period. If only one profile exists, the field displays that profile's name.

Example To list information about a specific profile, include its index on the command line:

```
admin> dir conn dallas
169 08/31/2002 22:21:07 dallas
```

Example To list all profiles types with a given string, use dir with the grep command:

```
admin> dir | grep -i ima
DS1-ATM          DS1 ATM/IMA line configuration parameters
IMA-GROUP-STAT   IMA group status
IMAGROUP         Inverse Multiplexing for ATM (IMA)group parameters
IMAHW-CONFIG     Inverse Multiplexing for ATM (IMA) HW parameters
LOAD-SELECT      Code images to load
<grep> Found 5 line(s) matching search criteria
```

See Also list, get, grep

dircode

Description Displays the contents of the PCMCIA flash memory card code directory. The flash cards contain code for the modules, run-time control module, and profiles. The system configuration is stored in the onboard nonvolatile RAM (NVRAM).

Permission level system

Usage dircode

The following error messages can appear when you use the dircode command:

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 starting 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.

Example

```
admin> dircode
Flash card code directory:
Card 1, format FTL/FAT, capacity 8MB
/current:
shelf-controller      1229934  Mon Jun  10 11:22:16 2002 Version 9.0a0e0
sdsl-atm-card         525661   Mon Jun  10 11:22:46 2002 Version 9.0a0e0
al-dmtadsl-atm-card  620347   Mon Jun  10 11:23:20 2002 Version 9.0a0e0
```

The information displayed by this command includes the card number (1 or 2) and the size of the code directory. For each expansion module installed in the system, it also shows the following information:

- The type of card the load is for
- The size of the code related to the card
- The date the load was copied to the flash card
- The code version

See Also format, fsck, load

dmtaldslines

Description Displays discrete multitone (DMT) Alcatel ADSL line use.

Permission level system

Usage dmtaldslines [-a | -d | -f | -sh | -sl | -u]

Command element Description

No options	Display the options for this command.
-a	Display all DMT Alcatel ADSL lines.
-d	Display all disabled DMT Alcatel ADSL lines.
-f	Display all free DMT Alcatel ADSL lines.
-sh shelf	Limit the output to lines on the specified shelf.
-sl shelf slot	Limit the output to lines on the specified slot.
-u	Display all Asynchronous Transfer Mode (ATM) DMT Alcatel ADSL lines in use.

Example To display all DMT Alcatel ADSL lines:

```
admin> dmtaldslines -a
All DMT Alcatel ADSL lines:
```

Line	{	1	4	1	}	(dvOp	dvUpSt	dvRq	sAdm	nailg)
		(Down	Idle	UP	UP	00151)				
Line	{	1	4	2	}	(Down	Idle	UP	UP	00152)
Line	{	1	4	3	}	(Down	Idle	UP	UP	00153)
Line	{	1	4	4	}	(Up	Idle	UP	UP	00154)
Line	{	1	4	5	}	(Down	Idle	UP	UP	00155)
Line	{	1	4	6	}	(Down	Idle	UP	UP	00156)

Line	{	1	4	7	}	(Down	Idle	UP	UP	00157)
Line	{	1	4	8	}	(Down	Idle	UP	UP	00158)
Line	{	1	4	9	}	(Down	Idle	UP	UP	00159)
Line	{	1	4	10	}	(Down	Idle	UP	UP	00160)
Line	{	1	4	11	}	(Down	Idle	UP	UP	00161)
Line	{	1	4	12	}	(Down	Idle	UP	UP	00162)

The data displayed includes the physical address of each line and the following status information:

Field	Description
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 operations mode.
sAdm	Desired administrative state of the line: ■ Down specifies that the line should terminate all operations and enter the deactivated state. ■ Up specifies that the line should be activated in normal operations mode. The 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 (for example, someone has dialed in) that should change the Stinger unit to the desired state.
nailg	Dedicated (nailed) group to which the line is assigned.

See Also sdsllines

dnstab

Description Displays the fallback Domain Name System (DNS) table, a local DNS host table used only when the regular name lookup fails. This table contains up to eight entries, each including a hostname and a list of the host IP addresses.

Permission level system

Usage `dnstab [-s] [entry number]`

Command element	Description
<code>-s</code>	Show the entire DNS host table.
<code>entry number</code>	Number of an entry in the DNS host table. Use this option to display a specific table entry.

Entering the command with no options displays the usage summary.

Example To display the entire DNS host table:

```
admin> dnstab -s
```

```
Local DNS Table: enabled, AutoUpdate: enabled.
```

```
Local DNS Table
```

	Name	IP Address	# Reads	Time of last read
1:	"wheelers"	206.65.212.9	*	- - -
2:	"foxhound"	1.0.0.1		- - -
3:	" "	-----		- - -
5:	" "	-----		- - -
6:	" "	-----		- - -
7:	" "	-----		- - -
8:	" "	-----		- - -

Field	Description
Local DNS Table	Whether enabled is set to yes in the <code>ip-global:dns-local-table</code> subprofile.
AutoUpdate	Whether auto-update is set to yes in the <code>ip-global:dns-local-table</code> 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.

Dependencies For the fallback table to be available, parameters must be configured in the `table-config` subprofile of the `dns-local-table` subprofile of the `ip-global` profile.

dslclstats

Description Displays statistics regarding the number of start, stop, and stream call-logging packets sent from a particular interface.

Permission level `system`

Usage dslclstats

This command can be run from any line interface module (LIM) or from the control module. When run from the control module, the command reports the counters for call-logging for trunk cards.

Example admin> dslclstats
DSL CL Start pkts sent = 7
DSL CL Stream pkts sent = 754
DSL CL Stop pkts sent = 3

dsllines

Description Displays the status of all DSL lines.

Permission level system

Usage dsllines [-a | -d | -f | -s | -sh | -sl | -u]

Command element	Description
-a	Show all DSL lines.
-d	Show disabled lines.
-f	Show all free lines.
-s	Show all lines summary.
-sh shelf	Limit the output to lines on the specified shelf.
-sl shelf slot	Limit the output to lines on the specified slot.
-u	Show in-use lines.

Example To show all free lines:

```
admin> dsllines -f
Free DSL lines:
Line      {      1  4  3  } (dvOp  dvUpSt  dvRq  sAdm  nailg  xDSL)
Line      {      1  4  4  } (Down  Idle   UP    UP    00153)
Line      {      1  4  4  } (Up    Idle   UP    UP    00154)
```

The data displayed includes the physical address of each line and the following status information:

Field	Description
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.

Field	Description
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 operations mode.
sAdm	Desired administrative state of the line: ■ Down specifies that the line should terminate all operations and enter the deactivated state. ■ Up specifies that the line should be activated in normal operations mode. The 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 (for example, someone has dialed in) that should change the Stinger unit to the desired state.
nailg	Dedicated (nailed) group to which the line is assigned.
xDSL	Type of DSL line.

Example To show a summary of all lines:

```
admin> dslines -s
```

Summary of All DSL lines:

Shelf	Slot	Lim-Type	Total-Port	Enabled-Port	Default-port
1	1	SDSL	48	48	0
1	2	SDSL	48	48	0
1	3	HDSL2	32	32	0

The data displayed includes the following fields:

Field	Description
Shelf	Shelf number of the LIM.
Slot	Slot number of the LIM.
Lim-Type	Type of LIM.
Total-Port	Total number of ports for this LIM.
Enabled-Port	Number of ports that are enabled.
Default-port	Number of ports with default settings.

dumpcachestat

Description Displays statistics about cache usage.

Permission level system

Usage dumpcachestat

Example

```
admin> dumpcachestat
Cache Updates 0      total 22
Cache Attempts 0     total 44
Cache Hits    0      total 22
Add count 321 Del count 216
Array Add count 0 Del count 0
Number of flash devices created 1 deleted 0
```

See Also ipcache

E

ether-display

Description Displays the contents of Ethernet packets.

Permission level diagnostic

Usage ether-display port# n

Command element	Description
port#	The Ethernet port on which the packets are received or transmitted. If you specify 0 (zero) for the port number, the Stinger unit displays all ports on the shelf.
n	The number of octets to display in each Ethernet packet.

Example To display Ethernet packet contents for port 0 in 12-octet sizes:

```
admin> ether-display 0 12
ETHER XMIT: 12 of 60 octets
10799E40: 08 00 20 75 80 6b 00 c0 7b 5e ad 3c .. u.k.. {^.<
ETHER RECV: 12 of 60 octets
1077D980: 00 c0 7b 5e ad 3c 00 80 c7 2f 27 ca ..{^.<... ./'.
ETHER XMIT: 12 of 509 octets
1079A480: 00 80 c7 2f 27 ca 00 c0 7b 5e ad 3c .../'... {^.<
ETHER XMIT: 12 of 330 octets
1079AAC0: 08 00 20 75 80 6b 00 c0 7b 5e ad 3c .. u.k.. {^.<
ETHER RECV: 12 of 60 octets
1077DFD0: 00 c0 7b 5e ad 3c 08 00 20 75 80 6b ..{^.<... u.k
ETHER XMIT: 12 of 451 octets
1079B100: 08 00 20 75 80 6b 00 c0 7b 5e ad 3c .. u.k.. {^.<
ETHER XMIT: 12 of 723 octets
1079B740: 00 20 af f8 0f 1d 00 c0 7b 5e ad 3c . .... {^.<
ETHER XMIT: 12 of 84 octets
1078F580: 08 00 20 75 80 6b 00 c0 7b 5e ad 3c .. u.k.. {^.<
ETHER RECV: 12 of 60 octets
1077E620: 00 c0 7b 5e ad 3c 00 20 af f8 0f 1d ..{^.<. ....
ETHER XMIT: 12 of 238 octets
1078FBC0: 00 20 af f8 0f 1d 00 c0 7b 5e ad 3c . .... {^.<
ETHER XMIT: 12 of 373 octets
10790200: 00 20 af f8 0f 1d 00 c0 7b 5e ad 3c . .... {^.<
ETHER RECV: 12 of 60 octets
1077EC70: 00 c0 7b 5e ad 3c 00 20 af f8 0f 1d ..{^.<. ....
ETHER XMIT: 12 of 267 octets
10790840: 00 20 af f8 0f 1d 00 c0 7b 5e ad 3c . .... {^.<
```

Example To stop displaying the Ethernet statistics, enter:

```
admin> ether-display 0 0
```



Note You must set debug to on for ether-display to have any effect

F

fatal-history

Description Displays the Stinger fatal-error log. Every time a fatal error occurs on a Stinger system, it is logged to the fatal-error history log. Available flash memory space limits the number of entries in the log. You can clear the log with the `clr-history` command.

Permission level system

Usage fatal-history

Example To display the fatal-history log:

```
admin> fatal-history
OPERATOR RESET: Index: 99 Revision: 1.3Ap6 Shelf 1
                  Date: 09/20/2002.      Time: 16:56:01
                  Reset from unknown, user profile super.
OPERATOR RESET: Index: 99 Revision: 1.3Ap6 Shelf 9
                  Date: 09/24/2002.      Time: 11:56:10
                  Reset from unknown, user profile super.
```

See Also `clr-history`

filtcache

Description Displays the number of times a cached RADIUS filter profile was used, and enables you to flush all filter cache buffers.

Permission level user

Usage `filtcache -s [filtername] | -f [-f]`

Command element	Description
<code>-s [filtername]</code>	If <code>filtername</code> is not specified, the command displays statistics for all cached filters. If it is specified, the command displays statistics only for the specified filter.
<code>-f [-f]</code>	Flush all cached filters. The second <code>-f</code> flag specifies that all filters are flushed without a prompt for confirmation being displayed.

Example The following command displays how many times a filter named `myfilter` has been used:

```
admin> filtcache -s myfilter
```

Filter Name	Time Created	Exp After (min)	Use Cnt	Refresh	Cache

myfilter	18:44:30	10	2	No	

The following command flushes all cached filters:

```
admin> filtcache -f
```

```
Flush all cached filter profiles? [y/n] y
```

```
All 3 cached RADIUS filter profiles flushed.
```

The following command displays how many times all cached RADIUS filters have been used:

```
admin> filtcache -s
```

Filter Name	Time Created	Exp After (min)	Use Cnt	Refresh	Cache

myfilter	20:01:50	1440	3	Yes	

filter-b	21:03:34	10	2	No	

filter-c	21:10:32	8	14	Yes	

See Also `filterdisp`

filterdisp

Description Enables you to display information about filters in use for active sessions.

Permission level `system`

Usage `filterdisp [sessNum ]`

Command element	Description
No options	Display all active sessions and their filter names.
<code>sessNum</code>	Display filter details for the specified session.

Example *Displaying all active sessions*

To display all active sessions and their filter names:

```
admin> filterdisp
ID   Username   Src Route-Filter Data-Filter Call-Filter TOS-Filter
-----
010  dialin-23  ext                a234567890123
016  dialin-4   ext                a234567890124
017  edleung    ext                a234567890125
018  jwebster   ext                a234567890126
019  pyan       loc                datfilt2    callfilt4   tostestfilt
020  guest      ext                a234567890123
021  pvc2       loc route-pvc                gen_callfilt
022  pvc4       loc                gen_callfilt
023  pvc5       loc
<end user list> 9 active user(s)
```

The output displays a session ID number, a username, and an indication of whether the session was authenticated locally. Sessions authenticated by local profiles display the filter names specified in the connection profile. Sessions authenticated by RADIUS display the filter names specified in the RADIUS profile. The fields in the command output provide the following information:

Field	Specifies
ID	Identification number for the session.
Username	Name of the authenticated profile.
Src	Whether the profile is downloaded through RADIUS (<i>ext</i>) or recognized as a local profile (<i>loc</i>).
Route-Filter	Whether a route filter has been applied to the session. For sessions authenticated locally, the name of the filter is supplied. For externally authenticated sessions, <i><filters present></i> indicates that a route filter has been applied. If blank, no route filter applies.
Data-Filter	Whether a data filter has been applied to the session. For sessions authenticated locally, the name of the filter is supplied. For externally authenticated sessions, <i><filters present></i> indicates that a data filter has been applied. If blank, no data filter applies.
Call-Filter	Whether a call filter has been applied to the session. For sessions authenticated locally, the name of the filter is supplied. For externally authenticated sessions, <i><filters present></i> indicates that a call filter has been applied. If blank, no call filter applies.
TOS-Filter	Whether a type of service (TOS) filter has been applied to the session. For sessions authenticated locally, the name of the filter is supplied. For externally authenticated sessions, the label <i><filters present></i> indicates that a TOS filter has been applied. If blank, no TOS filter applies.

Example To display the filter details for a particular session, specify the session ID as an argument on the `filterdisp` command line. (To obtain the session ID number, use the `filterdisp` command without an argument.) If you specify an invalid session number, the command returns an error. For example:

```
admin> filterdisp 3
Error: Invalid user session ID
```

Example The following sample output shows that no filters are applied to the sessions:

```
admin> filterdisp 23
Hostname:      pvc5
No associated filters

admin> filterdisp 10
Hostname:      dialin-4
No associated external filters
```

Example In the following sample output, call filters have been applied to a session that was authenticated locally:

```
admin> filterdisp 22
Hostname:      pvc4
Call Filter
Direction: In

Forward = no
Type = Generic Filter
offset = 0
len = 0
more = no
comp-neq = no
mask = 00:00:00:00:00:00:00:00:00:00:00:00
value = 00:00:00:00:00:00:00:00:00:00:00:00

Call Filter
Direction: Out

Forward = yes
Type = Generic Filter
offset = 0
len = 0
more = no
comp-neq = no
mask = 00:00:00:00:00:00:00:00:00:00:00:00
value = 00:00:00:00:00:00:00:00:00:00:00:00
```

Example The following sample output shows filters applied to an externally authenticated session:

```
admin> filterdisp 17
Hostname:      edleung
searching for external filters...
Externally obtained filters exist

Data Filter
Direction: Out

Forward = yes
```

```
Type = IP Filter
protocol = 0
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
destination-address-mask = 0.0.0.0
destination-address = 0.0.0.0
Src-Port-Cmp = none
source-port = 0
Dst-Port-Cmp = none
dest-port = 0
tcp-estab = no

Forward = yes
Type = Generic Filter
offset = 12
len = 2
more = no
comp-neq = no
dummyForPadding = 0
mask = ff:ff:00:00:00:00:00:00:00:00:00:00
value = 08:06:00:00:00:00:00:00:00:00:00:00
```

Dependencies The `filterdisp` command does not support virtual routers (VRouters) for externally authenticated sessions.

See Also `filtcache`

format

Description Formats a PCMCIA flash memory card, preparing it for use in a Stinger unit. You must format the card before you can use the `load` command to load code.

Permission level `code`

Usage `format [ -f | -o | -e | -b | -x ] [device]`

Command element	Description
-f	Force format without asking for verification.
-o	Format in version 2 old format.
-e	Erase the entire flash card.
-b	Format the flash card and reserve space for boot region.
-x	For ATA flash cards only, format without a Master Boot Record.
-e -b	Erase the boot region of a flash card.

Command element	Description
device	Name of the flash card to be formatted. The following are valid names: ■ [flash-card-]1 ■ [flash-card-]2 Device names can be abbreviated as 1 and 2.

The following error messages can appear when you use the `format` command

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 starting 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 currently in use (being read by a line interface or trunk module in LOAD state or being written as part of a code download).
LOG error, Shelf N, Controller-1, Time: hh:mm:ss-- ITP-1/12: _getPartData: _file_read(fd=5, ii->fragCnt=2925) FAILED	The flash card in the specified slot has not finished booting and as a result the format command has failed.

Example To format a PCMCIA flash memory card after inserting it in the second (righthand) slot in the control module:

```
admin> format flash-card-2
format will erase existing card 2 data; confirm: [y/n] y
```

See Also `dircode`, `fsck`, `load`

fsck

Description Audits inconsistent file conditions (which can include file contents) on a PCMCIA flash memory card.

For each file found, the command displays the type-name, type-number, decimal and hexadecimal byte counts, date written to flash memory, and whether blocks that were in use were allocated to a file. Any detected errors are reported. No errors are fixed.

Permission level code

Usage fsck [-b -c -v] device

Command element	Significance
-b	Ignore bad identifiers. Each flash card file system contains two directory blocks: an in-use block and an empty block used for deleting information. Both directory blocks contain an identifier that labels it a directory block. A <i>candidate</i> directory block is one that is missing the magic identifier but contains information that can be interpreted as directory-block information. If the <code>fsck</code> command finds no valid directory block but does find a candidate directory block, the <code>-b</code> option causes the system to ignore the missing identifier and use the candidate directory block anyway. The file system is to be used normally until the next reboot, assuming that the <code>fsck</code> command finds no other errors.
-c	Do not check file contents. By default, <code>fsck</code> checks the file contents for validity, which involves opening and reading every file, checking the file header, verifying the data length and CRC value, and performing other functions. This option causes <code>fsck</code> to check only the file-system format.
-v	Display verbose messages, including the number of blocks used, a block list, and (unless the <code>-c</code> option is specified) information about the files found.
device	Name of the flash card to be checked. The following are valid names: ■ [flash-card-]1 ■ [flash-card-]2 Device names can be abbreviated as 1 and 2.

Example To run a file-system check of the card named flash-card-1:

```
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 between 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: 2284
  Clusters lost during interrupted writes: 0
  Other reserved clusters: 1158
```

See Also dircode, format, load

h2>ftp

Description 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.

Permission level update

Usage ftp [-s source ip-address] [hostname] [port]

Command element	Description
-s source ip-address	Specify the source filename to transfer and IP address of the FTP server.
hostname	Specify the name of an FTP server.
port	Specify the server's FTP port value if it differs from the default value of 21.

Following are brief descriptions of `open` and the other FTP service commands:

Command element	Description
<code>ascii</code>	Sets the file transfer type for ASCII files.
<code>binary</code>	Sets the file transfer type so that files containing non-ASCII characters can be transferred correctly.
<code>bye</code>	Synonym for “quit”. Ends the FTP session and closes any open connections.
<code>cd [directory]</code>	Accesses a working directory named <code>directory</code> on the remote system.
<code>close</code>	Closes the connection with the remote system without exiting from FTP.
<code>debug</code>	Toggles debug output on and off.
<code>dir [directory]</code>	Synonym for <code>ls</code> . Displays a listing of <code>directory</code> on the remote system.
<code>exit</code>	Synonym for <code>quit</code> . Ends the FTP session and closes any open connections.
<code>get [remote filename] [local filename]</code>	Transfers a file named <code>remote filename</code> from the remote system to the local system. You can provide a remote file’s pathname as a valid remote filename. If you do not enter a <code>local filename</code> value, FTP transfers the file to the local current directory (LCD), using the remote filename. If you do not enter either a remote or local filename, you are prompted for both.
<code>hash</code>	Toggles the display of # as the progress indicator during file transfer.
<code>help</code>	Displays a list of commands recognized by the FTP client.
<code>lcd [directory]</code>	Sets the local current directory (LCD) to <code>directory</code> . If you do not enter a directory, the Stinger unit displays the current LCD to you.
<code>ls [directory]</code>	Synonym for <code>dir</code> . Displays a listing of <code>directory</code> on the remote system.
<code>open [hostname]</code>	Opens a connection to a remote system named <code>hostname</code> . If you do not specify a hostname, you are prompted for one.
<code>put [local filename] [remote filename]</code>	Transfers a file named <code>local filename</code> from the local system to the remote system. You can provide a local file’s pathname as a valid local filename. If you do not enter a <code>remote filename</code> value, FTP transfers the file to the remote system’s current working directory (CWD) using the local filename. If you do not enter either a local or remote filename, you are prompted for both.
<code>pwd</code>	Displays the pathname of the working directory on the remote system.

Command element	Description
quit	Synonym for <code>exit</code> . Ends the FTP session and closes any open connections.
set -s source ip-address	Sets options for a connection. You can display the options for the <code>set</code> command by entering <code>set ?</code>. In this release, the <code>set</code> command can be used only to set the source IP address of a connection using the <code>-s</code> option. The system uses the value specified with the <code>set -s</code> command instead of the value provided by the <code>system-ip-addr</code> parameter in the <code>ip-global</code> profile. Note If you are using <code>set</code> command, the client should not be connected to an FTP server.
user [username] [password]	Initializes a login to the host to which the FTP client is connected. If you do not enter a username or password, you are prompted to do so.



Note 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.

Usage `ftp [-s source ip-address]`
`//username:password@hostname:port/url-path/filename;type=a|i local-dir`

Command Element	Description
-s source ip-address	Specify the source filename to transfer and IP address of the FTP server.
username	Optional username. If the remote server requires a username, the system prompts you to enter one. Be sure to enter a colon (:) after any username you enter, and to omit the colon if you omit the username.
password	Optional password. If the remote server requires a password, the system prompts you to enter one. You must first enter a username to specify a password.
hostname	Fully qualified domain name of a network host, or the host's IP address in dotted decimal notation. If you use a domain name, use a fully qualified one as specified in Section 3.5 of RFC 1034, <i>Domain Names—Concepts and Facilities</i>, and Section 2.1 of RFC 1123, <i>Requirements for Internet Hosts—Application and Support</i>. A domain name is a sequence of domain labels separated by periods (.), starting and ending with an alphanumeric character, and optionally containing hyphens (-). In contrast to an IP address, the rightmost label can never start with a number.

Command Element	Description
port	Number of the port, in decimal notation, on an FTP host to which to connect. If you do not enter a port number, port defaults to 21. Be sure to enter a colon (:) before any port number you enter, and to omit the colon if you omit the port number.
url-path	Path on the remote system of one or more directory names to the file that you want to transfer. The slashes (/) that precede and follow the path are not part of the pathname(s). If you omit the path, be sure to retain both slashes.
filename	Name of the file on the remote host to transfer.
type=a i	Optional file transfer type: ■ Enter ;type=a to transfer ASCII files. ■ Enter ;type=i to transfer files containing non-ASCII characters, in binary mode. Note If you do not enter a type, the file transfer type defaults to binary mode. Be sure to enter a semicolon (;) before type, and to omit the semicolon if you do not enter a file transfer type.
local-dir	Optional path of one or more names to the local directory of flash memory where the Stinger unit is to store the transferred file. You can enter a PCMCIA slot number and a directory name (for example, 1/current). If you enter only a directory name, the unit uses the first slot with a file allocation table (FAT) formatted PCMCIA card. Be sure to include a space before local-dir.
	If you omit local-dir, the Stinger unit stores the file in the root directory of the first PCMCIA slot that contains a FAT-formatted flash card.

Example 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.
```

Example The following example 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.
```

Example The following example 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.
```

Dependencies To use the FTP client capability, your unit must have a 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.

G

gen-tone

Description Enables multiport tone tests for a range of line interface module (LIM) ports or a list of individual ports. The tests require that you connect an external test tone generator to the external or auxiliary port of a copper loop test (CLT) module or path selector module (PSM).

Permission level system

Usage gen-tone shelf slot
 ext start-port - end-port | p1 [p2. . . .]
 | aux start-port - end-port | p1 [p2. . . .]

Command element	Description
shelf	Shelf of the LIM whose ports are to be tested.
slot	Slot in which the LIM is located.
ext	Connection to the test tone generator is through the external port of a a CLT module or PSM.
aux	Connection to the test tone generator is through the auxiliary port of a CLT module or PSM.
start-port	First port of the range to be tested.
end-port	Last port of the range to be tested.
p1 [p2. . . .]	List of ports to be tested.

Example To test ports 1 through 10 for a LIM in shelf 1, slot 5 using the auxiliary port on a CLT module or PSM:
admin> gen-tone 1 5 aux 1 - 10

Example To test ports 3, 4, and 9 for a LIM in shelf 1, slot 5, using the auxiliary port on a CLT module or PSM:
admin> gen-tone 1 5 aux 3 4 9

Example To test ports 3 and 9 only for a LIM in shelf 1, slot 5, using the external port on a CLT module or PSM:
admin> gen-tone 1 5 ext 3 9

See Also degen-tone

get

Description Displays the contents of a profile or subprofile, but does not make it writable. Only the working profile can be modified. For information about reading a profile into the edit buffer to make it the working profile, see “read” on page 1-162.

The `get` command recognizes the period character (.) as shorthand for the working profile (the profile in the edit buffer).

Permission level system

Usage `get profile-type [profile-index] [[subprofile] [param-name
[param-index]]]`

Command element	Description
profile-type	Type of profile to be displayed, which might require an index as well. A period (.) represents the working profile (the profile in the edit buffer).
profile-index	Profile index (the name or address that distinguishes a profile from others of the same type). To see profile indexes, use the <code>dir</code> command.
subprofile	Subprofile within the specified profile.
param-name	Parameter within the specified profile. If the parameter is in a subprofile, you must specify the subprofile name first.
param-index	Complex parameters have an index. For example, the <code>interface-address</code> parameter contains both the <code>physical-address</code> and <code>logical-item</code> indexes.

Example *Displaying the contents of a profile*

To display the contents of a connection profile called `dallas`:

```
admin> get connection dallas
[in CONNECTION/dallas]
station*=dallas
active=yes
encapsulation-protocol=atm
called-number-type=national
dial-number=85283
clid=""
ip-options={ yes yes 1.1.1.1/8 0.0.0.0/0 7 100 255 no no 0 +
session-options={ "" "" no 120 no-idle 120 "" }
telco-options={ ans-and-orig no off 1 no no 64k-clear 0 "" "" +
answer-options={ }
usrRad-options={ global 0.0.0.0 1646 "" 1 acct-base-10 }
calledNumber=""
```

Example *Displaying the contents of a subprofile*

To display the ip-options subprofile in the connection profile called dallas:

```
admin> get connection dallas ip-options
[in CONNECTION/dallas:ip-options]
ip-routing-enabled=yes
vj-header-prediction=yes
remote-address=0.0.0.0/0
local-address=0.0.0.0/0
routing-metric=7
preference=100
down-preference=255
private-route=no
temporary-route=no
ip-direct=0.0.0.0
rip=routing-off
client-default-gateway=0.0.0.0
if-remote-address=0.0.0.0
tos-options={ no 00 normal input }
source-ip-check=no
```

Example *Displaying the contents of the working profile*

The get command, followed by a period (.), displays the contents of the current location in the working profile:

```
admin> get .
[in CONNECTION/dallas:ip-options]
ip-routing-enabled=yes
vj-header-prediction=yes
remote-address=0.0.0.0/0
local-address=0.0.0.0/0
routing-metric=7
preference=100
down-preference=255
private-route=no
temporary-route=no
ip-direct=0.0.0.0
rip=routing-off
client-default-gateway=0.0.0.0
if-remote-address=0.0.0.0
tos-options={ no 00 normal input }
source-ip-check=no
```

Example *Displaying a higher context than the current location*

You can add a space and two periods (..) to get . to display a higher context than the current location in the working profile:

```
admin> get . ..
[in CONNECTION/dallas]
station*=dallas
active=yes
encapsulation-protocol=atm
called-number-type=national
```

```
dial-number=""
clid=""
ip-options={ yes yes 10.122.99.1/24 0.0.0.0/0 7 100 255 no no +
session-options={ "" "" no 120 no-idle 120 "" 0}
telco-options={ ans-and-orig no off 1 no no 56k-restricted 0 +
usrRad-options={ global 0.0.0.0 1646 "" 1 acct-base-10 }
calledNumber=""
framed-only=no
atm-options={ aal5-llc 0 32 }
atm-connect-options={ aal5-llc 0 32 }
```

Example *Displaying a deeper context than the working profile*

To display a deeper context than the current location in the working profile, specify one or more subprofiles after the period:

```
admin> get . ip
[in CONNECTION/dallas:ip-options]
ip-routing-enabled=yes
vj-header-prediction=yes
remote-address=0.0.0.0/0
local-address=0.0.0.0/0
routing-metric=7
preference=100
down-preference=255
private-route=no
temporary-route=no
ip-direct=0.0.0.0
rip=routing-off
client-default-gateway=0.0.0.0
if-remote-address=0.0.0.0
tos-options={ no 00 normal input }
source-ip-check=no
```

Example *Displaying a parameter name or parameter index*

Use the param-name argument to display the IP address of an Ethernet interface:

```
admin> get ip-int {{1 c 1}0} ip-address
[in IP-INTERFACE/{ { shelf-1 controller 1 } 0 }:ip-address]
ip-address=10.65.12.224/24
```

Use the param-name param-index argument to display a complete physical address:

```
admin> get ip-int {{1 c 1}0} interface-address physical-address
[in IP-INTERFACE/{{shelf-1 controller 1} 0}:interface-address:
physical-address]
shelf=shelf-1
slot=controller
item-number=1
```

See Also list, read, write

gmac

Description Provide diagnostics on the Gigabit Ethernet (GigE) driver.

Permission level system

Usage gmac [-v | -i [-u | -d] | -n | -s | -l [-i | -e | -d | -p] -p | -r | -w | -d[-c | -a | -e] | -t | -?]

Command element	Description
-v	Show gmac version.
-i [-u/d]	With no additional option, initialize/reset the GigE port.
-u	Force GigE link up.
-d	Force GigE link down.
-n	Set up network processor to communicate with GMAC.
-s	Set up a SAR channel for communicating with GMAC.
-l [-i/e/d/p]	Loopback.
-i	Port set for internal loopback.
-e	Port set for external loopback.
-d	Port set for no loopback.
-p	Run loopback test for Ethernet power-on self test (POST).
-p	Ping test.
-r	Read a PHY register.
-w	Write to a PHY register.
-d [-c/a/e]	With no additional option, display all statistics.
-c	Clear GMAC statistics.
-a	Display ATM statistics.
-e	Display Ethernet statistics.
-t	Set debug level (0 through 3).
-?	Display a summary of commands.

Example Set up the network processor for communication with the GMAC:

```
admin> gmac -n
NP setup for gmac done.
```

Example Set up a SAR channel for communicating with the GMAC:

```
admin> gmac -s
GMAC: SAR conn. open with vpi = 0, vci = 200
```

Example Display the GMAC version:

```
admin> gmac -v
GMAC version : 0x0b
```

Example Reset the Gigabit Ethernet port:

```
admin> gmac -i
gigE port reset.
```

Example Display Gigabit Ethernet statistics:

```
admin> gmac -d -c
Clearing gmac stats.

admin> ping 201.168.53.122
PING 201.168.53.122 (201.168.53.122):
^C
--- 201.168.53.122 ping statistics ---
6 packets transmitted, 0 packets received
round-trip min/avg/max = 0/0/0 ms

admin> gmac -d
Gigabit Ethernet port statistics :
txOctetsLow      = 384
txOctetsHigh     = 0
txGoodPackets    = 6
txPkt64          = 6
txPkt65127       = 0
txPkt128255      = 0
txPkt256511      = 0
txPkt5121023     = 0
txPkt1024Max     = 0
txPktDefer       = 0
txPktUndSz       = 0
txUnderFlow      = 0
txPfcf           = 0
txPfcc           = 0
txRfcf           = 0
txRfcc           = 0
txOverFlow       = 0
txAlmostFull     = 0
rxOctetsLow      = 20965266
rxOctetsHigh     = 0
rxGoodPackets    = 15393
rxPkt64          = 0
rxPkt65127       = 0
rx128255         = 0
rx256511         = 0
rx5121023        = 0
rx1024Max        = 15393
rxMacType        = 0
rxCrcErrors      = 0
rxUnderSize      = 0
rxOverSize       = 0
rxAlmostFull     = 0
rxOverRun        = 0
rxMulticastPackets = 15392
rxBroadcastPackets = 0
...
```


gre

Description Displays Generic Routing Encapsulation (GRE) protocol statistics.

Permission level user

Usage gre c | z | k | s

Command element	Description
c	Display GRE counters.
z	Clear GRE counters.
k	Display the GRE key table.
s	Display GRE slot information.

Example To display GRE counters, use the gre c command:

```
admin> gre c
Received
  Total packets:      0
  Delivered locally:  0
    to slot/key:      0
    to slot/proto:    0
Transmitted
  Total requests:      0
  Packets sent:        0

PB stats:
  Received packets:    0      Delivered: 0
  Transmitted packets:0

Keys added: 0          Hits:    0
  deleted: 0           Misses: 0

CB msgs rcvd: 11       processed: 14
  sent: 21             generated: 21
```

Example To display the slots for which GRE is enabled, use the gre s command:

```
admin> gre s
Master shelf 1
Enabled slots:  1/3    1/13   1/7
```

grep

Description Filters the output of certain TAOS commands to make a specified pattern. The command is modeled on the `grep` command from the UNIX environment and has numerous applications in the TAOS operating system. The number of commands that support the `grep` capability changes as the functionality is integrated into the system. Following is a representative list of commands that currently support the `grep` feature:

```
arptable  
briChannels  
cadslLines  
callroute  
dadslLines  
dir  
ds3AtmLines  
filterdisp  
help  
if-admin  
ifmgr  
ipcache  
list  
modem  
oc3AtmLines  
ospf  
swanLines  
tlchannels  
uds3Lines  
userstat  
vdslchannels
```

Permission level user

Usage `command | grep [-c expression|-i expression] | -v expression]`

Command element	Description
<code>grep</code>	Displays only information that matches the expression pattern.
-c <code>expression</code>	Counts occurrences of the expression only. Does not display information.
-i <code>expression</code>	Uses pattern matching against the expression that is not case sensitive.
-v <code>expression</code>	Displays only information that does not match the expression pattern.

For the `expression` argument, the `grep` feature supports the following regular expressions, wildcard characters, and patterns:

Regular expression	Description
\ (backslash)	Turns off any special meaning of the following character.
. (period)	Matches any single character in the input string.
* (asterisk)	Matches zero or more occurrences of the previous character.
' ' (single quotation marks)	Enclose an expression to be matched.
""(double quotation marks)	Enclose a pattern that contains spaces or other quotation marks.
^ (circumflex)	Specifies the beginning of a line.
\$ (dollar sign)	Specifies the end of line.
(vertical bar)	Specifies a logical OR relationship.
[] (square brackets)	Specifies any one of the characters in a range.
() (parentheses)	Identifies group expressions

To search for a character that is a wildcard, you must precede it with the backslash character, even if the wildcard character is within the boundaries of quotation marks.

The output data from the command is scanned line by line. If the pattern you specify is encountered in the line, that line is displayed. If you use the `-c` argument, the number of lines found matching the pattern are counted and displayed at the end of the command. Note that the field headers and footers might be omitted from the display if they do not match the pattern. However, error messages are exempt from pattern matching.



Note If you use the `grep` feature with a command that does not support filtering, the system does not display an error. Instead, the command output is simply not filtered.

Example Following are two uses of the `grep` command related to virtual links and soft permanent virtual circuits (SPVCs):

```
admin> ? | grep atm
atmvccstat ( system )
atmvcl ( system )
atmvcx ( system )
atmvpl ( system )
atmvpx ( system )

admin> ? | grep spv
spvcc ( system )
spvcstat ( system )
spvpc ( system )
```

See Also `?`, `dir`

gunzip

Description The gunzip command uncompresses files on the flash card that have been compressed by the gzip command. This command functions in the same way as the UNIX gunzip command, and performs the same function as the gzip command used with the -d option.

Permission level system

Usage gunzip [-options] file

Command element	Description
-V	Toggle verbose mode
-t	Time the compression operation

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

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

Dependencies This command can be used only if the allow-system parameter is set to yes in the user profile.

gzip

Description The gzip command compresses files on the flash card. This command functions in the same way as the UNIX gzip command.

Permission level system

Usage gzip [-options] file

Command element	Description
-d	Decompress the specified file(default for 'gunzip')
-1 to -9	Set the compression level (-1 : fastest; -9 : best)
-f	Compress using Z_FILTERED
-h	Compress using Z_HUFFMAN_ONLY
-V	Toggle verbose mode
-t	Time the compression operation

Example 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
```

Dependencies This command can be used only if the allow-system parameter is set to yes in the user profile.

H

hds12lines

Description Displays the port status and dedicated (nailed) group for each HDSL2 port.

Permission level System

Usage hds12lines [-a | -d | -f | -u | -sh | -sl | -t]

Command element	Description
-a	Show all HDSL2 lines.
-d	Show disabled lines.
-f	Show all free lines.
-u	Show in-use lines.
-sh shelf	Limit the output to lines on the specified shelf.
-sl shelf slot	Limit the output to lines on the specified slot.
-t	Toggle debug flag.

Example To display all lines for the first 16 ports on an HDSL2 module in slot 4:

```
admin> hds12 -a
```

All HDSL2 lines:

	dvOp	dvUpSt	dvRq	sAdm	na1lg)
Line { 1 4 1 }	(Down	Idle	DOWN	DOWN	00151)
Line { 1 4 2 }	(Down	Idle	DOWN	DOWN	00152)
Line { 1 4 3 }	(Up	Idle	UP	UP	00153)
Line { 1 4 4 }	(Down	Idle	DOWN	DOWN	00154)
Line { 1 4 5 }	(Down	Idle	DOWN	DOWN	00155)
Line { 1 4 6 }	(Down	Idle	DOWN	DOWN	00156)
Line { 1 4 7 }	(Up	Idle	UP	UP	00157)
Line { 1 4 8 }	(Down	Idle	DOWN	DOWN	00158)
Line { 1 4 9 }	(Up	Idle	UP	UP	00159)
Line { 1 4 10 }	(Up	Idle	UP	UP	00160)
Line { 1 4 11 }	(Down	Idle	DOWN	DOWN	00161)
Line { 1 4 12 }	(Down	Idle	DOWN	DOWN	00162)
Line { 1 4 13 }	(Up	Idle	UP	UP	00163)
Line { 1 4 14 }	(Down	Idle	DOWN	DOWN	00164)
Line { 1 4 16 }	(Down	Idle	DOWN	DOWN	00166)

Field	Description
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.

Field	Description
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 operations 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. The 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 that should change the Stinger unit to the state desired.
nailg	Dedicated (nailed) group to which the line is assigned.

help

Description Displays a list of all available commands or help text about a specific command. The question-mark (?) is a shortcut version of this command.

Permission level user

Usage help [-a] | [command-name]

Command element	Description
-a	List all commands. (Without this option, the list includes only commands authorized by the current user profile.)
command-name	Display information about the specified command.

Example To display a list of commands authorized for your current login:

```
admin> help
?                ( user )
arp              ( system )
auth             ( user )
clear            ( user )
clock-source     ( diagnostic )
clr-history      ( system )
```

```

connection          ( system )
date                 ( update )
delete               ( update )
device               ( diagnostic )
dir                  ( system )
dircode              ( system )
ether-display        ( diagnostic )
fatal-history         ( system )
format               ( code )
get                  ( system )
help                 ( user )
if-admin              ( diagnostic )
line                 ( system )
[More? <ret>=next entry, <sp>=next page, <^C>=abort]

```

Example To display help text about the dir command:

```

admin> help dir
dir                  list all profile types
dir profile-type     list all profiles of the specified type
dir profile-type profile-index list the specified profile instance

```

Dependencies The current security level is set by the current user profile and determines which commands are displayed in response to this command. If the current user profile does not have sufficient privileges to run a command, the command is not displayed unless you specify the -a option. By default, commands that go with the current user security level are always displayed.

See Also auth

history

Description The history command displays command logs to the terminal session.

Permission level user

Usage history

Example Following is a sample output of the history command, followed by a description of the fields in the output:

```

admin> history
Date      Time      Source      User      Id Card      Command
11/13/2003 16:31:00 console     admin     01 {01 08} history
11/13/2003 16:30:52 135.17.134.39 user2     03 {01 08} quit
11/13/2003 16:30:49 135.17.134.39 user2     03 {01 08} save c log
11/13/2003 16:30:41 135.17.134.39 user2     03 {01 08} dir cmd-log
11/13/2003 16:30:32 135.17.134.39 user2     03 {01 08} help
11/13/2003 16:30:29 135.17.134.39 user2     03 {01 08} atmccastat
11/13/2003 16:30:25 135.17.134.39 user2     03 {01 08} show
11/13/2003 16:30:16 135.17.134.39 user1     02 {01 08} quit
11/13/2003 16:30:07 135.17.134.39 user1     02 {01 08} history
11/13/2003 16:29:58 135.17.134.39 user1     02 {01 08} dir

```

Field	Description
Date	Date the command was entered.
Time	Time the command was entered
Source	How the user initiated the session, for example, via telnet or by connecting to the serial port.
User	The user profile associated with the user who entered the command.
Id	User session ID number.
Card	Shelf and slot number from which the command was entered.
Command	Command entered by the user.

I

if-admin

Description Displays information about or specifies the state of a Simple Network Management Protocol (SNMP) interface.

Each device in the system has a unique SNMP interface number assigned to the device when a module is installed. Interface numbers are stored in nonvolatile RAM (NVRAM), which is not affected by system resets. A physical device keeps the same interface number across system resets or power failures.

Permission level diagnostic

Usage if-admin -a | -d interface| -l | -u interface| -r interface

Command element	Description
-a	List available SNMP interface numbers.
-d interface	Administratively disconnect a specified SNMP interface
-l	List SNMP interface and device address mappings.
-u interface	Administratively turn on a specified SNMP interface.
-r interface	Reset an SNMP interface.

Example To display a list of all SNMP interface numbers assigned by the system, specify the -l option:

```
admin> if-admin -l
SNMP-IF  DEVICE ADDRESS
  101    -   { 1 11 32 }
    1    -   { 1 17 1  }
  102    -   { 1 11 33 }
    2    -   { 1 3 1  }
```



```
103 - { 1 11 34 }
3 - { 1 3 2 }
104 - { 1 11 35 }
4 - { 1 3 3 }
105 - { 1 11 36 }
5 - { 1 3 4 }
106 - { 1 11 37 }
6 - { 1 3 5 }
107 - { 1 11 38 }
7 - { 1 3 6 }
108 - { 1 11 39 }
8 - { 1 3 7 }
[More <ret>=next entry, <sp>=next page, <^C>=abort]
```

```
To turn on SNMP interface number 111:
admin> if-admin -u 111
interface 111 state change forced
```

if-trap-admin

Description With the if-trap-admin command, you can change the setting of the desired-trap-trap parameter for all admin-state-phys-if profiles, admin-state-perm-if profiles or both admin-state-phys-if and admin-state-perm-if profiles.

Permission level update

Usage if-trap-admin [-a | -s | -m] state

Command element	Description
-a	Change trap settings for all profiles (ADMIN-STATE-PHYS-IF and ADMIN-STATE-PERM-IF)
-s	Change trap settings for ADMIN-STATE-PHYS-IF profile
-m	Change trap settings for ADMIN-STATE-PERM-IF profile
state	Select one of, system (the default), enable, or disable.

Example The following sample commands change the setting of the desired-trap-state for all slots in the system to system-defined:

```
admin> if-trap-admin -a system
Massive desired-trap-state change done
```

igmp

Description Displays multicast information about Internet Group Management Protocol (IGMP) groups and clients.

Permission level system

Usage `igmp [mbone | groups | clients | slots | vc ] [profile [mcast-profile] | delete [grp_addr] [if_num] ] [smbone | sgroups [bridgeNum] | sclients [bridgeNum] ] [slots | sdelete [bridgeNum] [grp_addr] [if_num] ]`

Command element	Description
mbone	Display multicast mbones (backbones).
groups	Display active multicast group addresses and interfaces.
clients	Display multicast clients.
slots	Display multicast enable slots.
vc	Display the multicast VCs that are configured and active.
profile	Display multicast profiles.
delete	Delete the client.
smbone	Display all snooping MBONE interfaces, or the snooping MBONE interface for the specified bridge group.
sgroups	Display all multicast groups joined within a specified bridge group.
sclients	Display the IGMP clients for a specified bridge group.
slots	Display the slots using IGMP snooping.
sdelete	Delete the groups joined through the trunk module.



Note For the following examples, the MBONE interface is on the Gigabit Ethernet port and the clients are on a trunk interface (a remote client), and on ADSL LIM slots 1 and 5.

Example Display multicast clients:

```
admin> igmp client
IGMP Clients
  Client          Version    RecvCount    CLU    ALU
  1 (Mbone)       2          0            0      0
  14              2          0            0      0
```

The output contains the following fields:

Field	Description
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.

Field	Description
Version	IGMP version.
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.

Example Display active multicast group addresses and interfaces:

```
admin> igmp group
IGMP Group address Routing Table
Up Time: 0d 0:13:52
Group Address      Members      Expire time      Counts
230.0.0.9          14           00:00:31         0 :: 0 S4
* (Mbone)          0 :: 0 S4
Slot 1:5
Slot 1:2
```

The output contains the following fields:

Field	Description
Group address	Multicast address used for the group. An asterisk indicates the IP multicast address being monitored. If a group has no members, the system forwards multicast traffic for the group to the MBONE interface (the default route).
Members	Interface ID of multicast group members.
Expire time	When this membership expires. The system sends out IGMP queries every 60 seconds, so the expiration time is usually renewed. If the expiration time is reached, the system 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.
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.

Example Display information about slots supporting IGMP clients:

```
admin> igmp slot
IGMP Client Slots
Shelf:Slot      Group      SendCount
1:8             230.0.0.9      0
1:5             230.0.0.9      0
1:2             230.0.0.9      0
```

The output contains the following fields:

Field	Description
Shelf:Slot	Shelf and slot card the MBONE connection is on.
Group	Interface number of connection.
SendCount	Number of packets sent across the interface.

Example Display information about multicast service profiles:

```
admin> igmp profile
```

```
IGMP Service Profiles
```

```
Service Name           : test
Filter Type            : MCAST_FILTER_INCLUSIVE
Filter List( Group Range) :
                        235.1.1.1 - 235.1.1.1 ( Count = 1 )
```

The output contains the following fields:

Field	Description
Service Name	Name of the multicast service profile.
Filter Type	Inclusive or exclusive multicast group filtering in the named profile.
Filter List	Multicast group addresses to be filtered.

Example Display information about the current MBONE interface:

```
admin> igmp mbone
Mbone is currently:
Slot 1:8 ifNum = 1
```

imagroups

Description Displays the status of any groups of E1 or T1 interfaces configured in inverse multiplexing over ATM (IMA) mode that are in use, free, or disabled, on any line interface modules (LIMs) in a Stinger unit.

Permission level system

Usage imagroups [-a | -d | -f | -u]

Command element	Description
No options	Display the options for this command.
-a	Show all IMA groups.
-d	Show disabled groups.
-f	Show all free groups.
-u	Show groups that are in use.

Example To display all IMA groups:

```
admin> imagroups -a
All IMA groups:
ima-co { 1 2 25 } (dvOp dvUpSt dvRq sAdm nailg)
                  (Down Idle UP UP 100)
```

Field	Description
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 operations 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. The 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 that should change the Stinger unit to the state desired.
nailg	Dedicated (nailed) group to which the line is assigned.

imalines

Description Displays the status of all T1 or E1 lines, or those that are in use, free, or disabled, on any line interface modules (LIMs) in a Stinger unit.

Permission level system

Usage imalines [-a | -d | -f | -u]

Command element	Description
No options	Display the options for this command.
-a	Show all inverse multiplexing over ATM (IMA) lines.
-d	Show disabled lines.

Command element	Description
-f	Show all free lines.
-u	Show lines that are in use.

Example To display the status of all IMA lines:

```
admin> imalines -a
```

All IMA lines:

		(dvOp	dvUpSt	dvRq	sAdm	lMode	Nailg)
Line {	1 3 1 }	(Up	Assign	UP	UP	IMA	00101)
Line {	1 3 2 }	(Up	Assign	UP	UP	IMA	00101)
Line {	1 3 3 }	(Up	Assign	UP	UP	IMA	00101)
Line {	1 3 4 }	(Down	Idle	DOWN	DOWN	ATM	00104)
Line {	1 3 5 }	(Down	Idle	DOWN	DOWN	ATM	00105)
Line {	1 3 6 }	(Down	Idle	DOWN	DOWN	ATM	00106)
Line {	1 3 7 }	(Down	Idle	DOWN	DOWN	ATM	00107)
Line {	1 3 8 }	(Down	Idle	DOWN	DOWN	ATM	00108)

Field	Description
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 operations 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. The 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 that should change the Stinger unit to the state desired.

Field	Description
lMode	Interface mode: ■ IMA indicates an interface that is part of an IMA group. ■ ATM indicates a single, ungrouped interface. Both IMA and ATM interface types can support User-to-Network Interface (UNI) or Private Network-to-Network Interface (PNNI) signaling.
nailedg	Dedicated (nailed) group to which the line is assigned.

See Also imagroups

info

Description info displays some useful system information.

Permission level system

Usage info info-type [port/conn-id/slot] [ifnum]

Command element	Description
info-type	Type of information to display. Specify one of the following: ■ conn—Information about active connections. ■ aal5—AAL5 channel information. ■ atm—Utopia port information. ■ ether—Ethernet port or device information.
port	Port number.
conn-id	Connection ID
Slot	Slot number of the device.
ifnumb	Interface number.

Example Without any arguments, info displays some useful system information.

```
admin> info
Platform           : Lucent Stinger FS
System Name        : (not configured)
Serial Number      : 1308530130
Software Version   : TAOS 9.5-206.0e0 (stngrcm2)
* * * rtr/stngrcm2 <rsshukla> Jul 11 2003 17:57 * * *
Boot Version       : TAOS 9.5-206.0e0
Controller Role    : Primary
Hardware revision: 2.2 Model E - IP (Version B) with gigE fiber interface.
```

Example The `info conn` command displays information about active connections.

Without any arguments, the `info conn` command reports information on all connections on the Fast Ethernet trunk module. For example:

```
admin> info conn
slot if      type vpi/vci IW
-----
6    17      ATM  0/131  VBR
17   1       CTL  0/123  VBR
17   2       CTL  0/124  VBR
17   65534   ETH  0/0    VBR
17   65535   ETH  0/0    VBR
```

To display detailed information about a specific connection, append the interface number and the slot number to the `info conn` command. For example, the following command displays information about the connection on interface 17 on slot 6:

```
admin> info conn 17 6
Interface           : 17
Slot                : 6
Interface Dir       : TOWARDS LIMS
Connection Type     : VLAN BRIDGING
MTU                 : 1610
WINPATH ATM INFO    :
rx Utopia Port      : 0
rx Utopia Address   : 0
rx Utopia VPI       : 0
rx Utopia VCI       : 131
tx Utopia Port      : 0
tx Utopia Address   : 0
tx Utopia VPI       : 0
tx Utopia VCI       : 131
ATM Encap Type      : ATM_ENCAP_ILC
IW Mode             : IW MODE BRIDGING
qosType             : 3
pcr                 : 0
scr                 : 0
mbs                 : 0
cdvt                : 0
VLAN INFO vlan id   : 66
VLAN INFO acceptTagged : 0
VLAN INFO acceptUnTagged: 1
atmChannel          : 22
etherInfo IWMode     : IW MODE BRIDGING
VLAN INFO vlan id   : 0
VLAN INFO acceptTagged : FALSE
VLAN INFO acceptUnTagged: FALSE
Ether-QosInfo packetrate: 0
```


inputrelaytest

Description The `inputrelaytest` command simulates the status of relays to generate relay alarm and trap conditions for testing.

Permission level system

Usage `inputrelaytest [ -p | -i | -m | -(0-7) | -t | -s -h]`

Command element	Description
-p	Enables/disables the input relay alarm test. When you have completed the test, you must enter the <code>inputrelaytest -p</code> 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.
-h	Help

Example 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
```

Example 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
```

Example 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!
```

Example The following commands close all relays:

```
admin> inputrelaytest -m
Set relay CLOSED mode
admin> inputrelaytest -0
All test input relay closed
```

Example The following commands simulates an individual input relay, relay 1, as open:

```
admin> inputrelaytest -m
Set relay OPEN mode
admin> inputrelaytest -1
Test input relay 1 open
```

Example 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
```

Example The following command 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
```

ipcache

Description A utility that displays, debugs, enables, and disables the IP route cache.

Permission level system

Usage ipcache [-r vroutername] cache | debug | disable | enable

Command element	Description
-r vroutername	Name of the virtual router (VRouter). If you do not specify a name, the system uses the global VRouter.
cache	Display the cache.
debug	Enable or disable debugging
disable	Disable IP route cache routing on module. Enabled by default. Available only on modules.
enable	Enable IP route cache routing on module. Available only on modules.

Example To display output on the control module:

```
admin> ipcache cache
Hsh      Address      Gateway      Ifname      Sh/Sl/T      MTU
20       50.0.0.20      200.168.26.74  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
```

Field	Description
Hsh	Hash code.
Address	Destination IP address.
Gateway	IP address of the gateway.
Ifname	Interface name.
Sh/Sl/T	- Sh is an abbreviation for <i>shelf</i>. - Sl is an abbreviation for <i>slot</i>. - Type (T) is either D (dynamic cache entry) or S (static cache entry).
MTU	Maximum transmission unit.
MPath	Displays cache entries derived from multipath routes. If Y is displayed, the route is listed.

Example To display output on a module in slot 3:

```
admin> open 1 3
ether2-1/3> ipcache cache
```

Hsh	Address	Gateway	Sh/Sl/T	Switched	MTU	MPath
0	99.1.1.1	200.168.21.30	1/14/D	0	1524	Y/0.0.0.0/0
20	50.0.0.20	200.168.28.170	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

See Also `dumpcachestat`, `iproute`

ip-pools

Description

Permission level

Usage `ip-pools [-r VRoutername]`

Command element	Description
<code>-r VRoutername</code>	To display IP pool information for a specific virtual router (VRouter), replace <code>VRoutername</code> with the name of a VRouter. If you do not specify a VRouter name, the system assumes the global VRouter.

Example The following example displays the status of global address pools. The output shows two configured pools, with the base address, address count, and number of addresses in use for each pool:

```
admin> ip-pools
```

Pool#	Base	Count	InUse
1	192.168.0.0	10	0
2	10.0.0.0	1000	0

Number of remaining allocated addresses: 0

Example The following example is for a VRouter `vrtr1`:

```
admin> ip-pools vrtr1
```

Pool#	Base	Count	InUse
1	20.0.0.0	100	0

Number of remaining allocated addresses: 0

ipportmap

Description Displays active User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) port mappings.

Permission level system

Usage ipportmap -c | -m

Argument	Description
-c	Display the cache state.
-m	Display current mappings.

Example To display the number of active ports:

```
admin> ipportmap -c
Port Counts
Active Ports: 18
Active UDP Ports: 17
Active TCP Ports: 1
IP Port Cache is ON
```

Example To display the protocol, IP address, shelf number, and slot number for each port:

```
admin> ipportmap -m
```

Port	Proto	Addr	Sh/Sl/ID/TAG	Refcnt	ICMP	PCB
23	TCP	0.0.0.0/32	1/42/0 /0	1066	803b4550	
11107	UDP	0.0.0.0/32	1/7 /0 /ffffffff	3	0	
9212	UDP	0.0.0.0/32	1/7 /0 /ffffffff	3	0	
1018	UDP	0.0.0.0/32	1/7 /0 /ffffffff	3	0	
9213	UDP	127.0.0.1/32	1/42/0 /0	3	0	
9214	UDP	0.0.0.0/32	1/8 /0 /ffffffff	3	0	
1019	UDP	0.0.0.0/32	1/8 /0 /ffffffff	3	0	
3350	UDP	0.0.0.0/32	1/42/0 /0	3	0	
1701	UDP	0.0.0.0/32	1/42/0 /0	3	0	
1020	UDP	0.0.0.0/32	1/42/0 /0	3	0	
5150	UDP	0.0.0.0/32	1/42/0 /0	3	0	
161	UDP	0.0.0.0/32	1/42/0 /0	3	0	
123	UDP	0.0.0.0/32	1/42/0 /0	3	0	
7	UDP	0.0.0.0/32	1/42/0 /0	3	0	
520	UDP	0.0.0.0/32	1/42/0 /0	3	0	
1021	UDP	0.0.0.0/32	1/42/0 /0	3	0	
1022	UDP	0.0.0.0/32	1/42/0 /0	3	0	
1023	UDP	0.0.0.0/32	1/42/0 /0	3	0	

iproute

Description Enables you to manually add or delete IP routes. Changes to the routing table do not persist across system resets.

Permission level system

Usage iproute

```
[add dest_IPaddr[/subnet_mask] gateway_IPaddr[/subnet_mask] [pref] [metric]  
|delete dest_IPaddr/subnet_mask [gateway_IPaddr[/subnet_mask]]]
```

Command element	Description
add	Add an IP route to the routing table.
delete	Delete an IP route from the routing table.
dest_IPaddr/subnet_mask	Destination network address and optional subnet mask (in bits). The default is 0.0.0.0/0.
gateway_IPaddr/subnet_mask	IP address of the router that can forward packets to the destination network, and optional subnet mask (in bits). The default is 0.0.0.0.
pref	Route preference. The default is 100.
metric	Virtual hop count of the route. You can enter a value between 1 and 15. The default is 1.

Example To add a static IP route to the unit's routing table, use the `iproute add` command. For example, the following command adds a route to the 10.1.2.0 network, 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 replaces the existing route only if it has a higher metric than the route you are attempting 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.



Note Routing Information Protocol (RIP) updates can change the metric for the route. Also, any routes you add with the `add` option are lost when you reset the Stinger unit.

Example To remove a static IP route from the unit's routing table, enter the `iproute delete` command. For example, the following command removes the route to the 10.1.2.0 network:

```
admin> iproute delete 10.1.2.0/24 10.0.0.3/24
```



Note RIP updates can add back any route you remove with `delete` option. Also, the Stinger unit restores all routes listed in the `ip-route` profile after a system reset.

See Also `ipcache`

isolate

Description Enables galvanic isolation tests for a range of line interface module (LIM) ports or a list of individual ports.

Permission level system

Usage isolate shelf slot start-port - end-port | shelf slot p1 [p2. . . .]

Command element	Description
start-port	First port of the range to be tested
end-port	Last port of the range to be tested
p1 [p2. . . .]	List of ports to be tested

Example To test ports 1 through 10 for a LIM in shelf 1, slot 5:

```
admin> isolate 1 5 1 - 10
```

To test ports 3, 4, and 9 for a LIM in shelf 1, slot 5:

```
admin> isolate 1 5 3 4 9
```

See Also deisolate

L

line

Description Specifies that the upper-right or lower-right portion of the status window (or both) displays line and channel status information. If the status window is not already displayed, this command opens it with the connection status information displayed.

Permission level system

Usage line all | enabled | top | bottom

Command element	Description
all	Display status information about all lines.
enabled	Display status information only about enabled lines.
top	Display line status in the upper portion of the status window.
bottom	Display line status in the lower portion of the status window (the default).

Example To display line status information in the upper part of the status window:

```
admin> line top
```

```

2 Connections
001 tomw TCP 1/7/14 19200 SanFran+ 1/13/8 RA I.....
002 timl TCP 1/7/3 56000 Berkeley 1/01/04 RA N.....
                                1/01/05 RA T.....
                                CleveLa+ 1/01/01 RA T.....
                                Oakland 1/01/02 RA S.....

M: 48 L: info Src: shelf-1/controller

Issued: 16:48:02, 09/27/2002
```

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

Line status information includes the following identifiers and codes:

- A line identifier in shelf/slot/line format.
- A two-character code indicating the line's link status.
- A single-character code indicating channel status. For Signaling System 7 (SS7) data trunk, this character code is always 7.

Following are the link-status codes:

Link-status code	Description
LS (UDS3 lines)	Loss of signal. No signal has been detected.
LF (UDS3 lines)	Loss of frame. A signal is present but is not valid for framing.
RA	Red Alarm. The line is not connected, or it is improperly configured, experiencing a very high error rate, or supplying inadequate synchronization.
YA	Yellow Alarm. The Stinger unit is receiving a Yellow Alarm pattern, which indicates that the other end of the line cannot recognize the signals the Stinger unit is transmitting.
DF	D-channel fail. The D channel for a PRI line is not currently communicating.
1S	All ones. The network is sending a keepalive signal to the Stinger unit to indicate that the line is currently inoperative.
DS	Disabled. The line might be physically connected, but the profile specifies that it is inactive.

Following are the channel-status codes:

Channel status code	Description
.	The channel is not available for one of the following reasons: ■ The line is disabled. ■ The channel has no physical link or does not exist. ■ The channel configuration specifies that the channel is unused. ■ The channel is reserved for framing.
*	The channel is connected in a current call.
-	The channel is currently idle, but in service.
c	The channel is currently not available because it is in the process of clearing the most recent call, or because it is in the process of sending echo cancellation tones to receive a call.
d	The Stinger unit is dialing from this channel for an outgoing call.
r	The channel is ringing for an incoming call.
m	The channel is in maintenance/backup mode (ISDN and SS7 only).
n	The channel is dedicated (nailed).
o	The channel is out of service (ISDN and SS7 only).
s	The channel is an active D channel (ISDN only).

See Also connection, log, view

list

Description Lists the contents of the current or specified context in the working profile. Listing a subprofile changes the current context to that subprofile. Specifying two periods (..) as the command argument changes the current context back to one level higher in the working profile (making the subprofile inactive). The `list` command works only on the working profile.

Permission level system

Usage list [...] [param-name [param-index] [subprofile]]

Command element	Description
.. (two periods)	Close the current subprofile, return to the previous higher context, and list it. You can also enter list .. with the name of a subprofile from the higher context—for example, list .. ip-options. In this way the single entry of the command switches the context and lists the specified subprofile.
param-name	List a parameter in the current context. If the parameter is in a subprofile, you must specify the subprofile name first.
param-index	List complex parameters that have an index. For example, the interface-address parameter contains both the physical-address and logical-item indexes.
subprofile	List the contents of a subprofile that is visible in the current context, and make that subprofile the current context.

Example To make a connection profile named dallas the working profile:

```
admin> read connection dallas
```

To list its contents:

```
admin> list
[in CONNECTION/dallas]
station*=dallas
active=yes
encapsulation-protocol=atm
called-number-type=national
dial-number=85283
clid=""
ip-options={ yes yes 1.1.1.1/8 0.0.0.0/0 7 100 255 no no 0 +
session-options={ "" "" no 120 no-idle 120 "" }
telco-options={ ans-and-orig no off 1 no no 64k-clear 0 "" "" +
usrRad-options={ global 0.0.0.0 1646 "" 1 acct-base-10 }
calledNumber=""
```

To list the ip-options subprofile:

```
admin> list ip-options
[in CONNECTION/dallas:ip-options]
ip-routing-enabled=yes
vj-header-prediction=yes
remote-address=0.0.0.0/0
local-address=0.0.0.0/0
routing-metric=7
preference=100
down-preference=255
```

```

private-route=no
temporary-route=no
ip-direct=0.0.0.0
rip=routing-off
client-default-gateway=0.0.0.0
if-remote-address=0.0.0.0
tos-options={ no 00 normal input }
source-ip-check=no

```

To return to the top-level context of the profile:

```
admin> list ..
```

To use the list command to display the telco-options subprofile:

```

admin> list .. telco
[in CONNECTION/dallas:telco-options]
answer-originate=ans-and-orig
nailed-groups=1
force-56kbps=no
data-service=56k-restricted
call-by-call=0
billing-number=""
transit-number=""

```

The list command works only on the working profile. To make an existing profile the working profile, use the read command. When you create a new profile, it becomes the working profile automatically.

See Also dir, get, read, new, set, write

load

Description Uploads a code image to flash memory 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 Trivial File Transfer Protocol (TFTP), or on the PCMCIA flash memory card file system of the control module.

Permission level update

Usage load [-v] [-l] [-t] [-e password] load-type [subtype] source
[target-device]

Command element	Description
-v	Display verbose output for configuration loads.
-l	Load the code to the local controller only and do not transfer the image to the peer.
-t	Load the peer control module as well as the current control module.

Command element	Description
<code>-e password</code>	Password to generate a key for encryption or decryption. This option supports only a load type of config using a source of network.
<code>load-type</code>	Type of the image to upload. If no load type is specified, the load types that reside on the source device are loaded. Following are valid values: ■ <code>config</code>—Configuration file ■ <code>file</code>—Generic file. ■ <code>boot-cm</code>—Control module boot image. ■ <code>tar</code>—Software binaries. ■ <code>gzip</code>—Compressed binaries. ■ <code>cm</code>—Control module image. ■ <code>cm-v2</code>—Code for the new control modules. ■ <code>sdsl-atm</code>—Code for an SDSL LIM. ■ <code>al-dmtadsl-atm</code>—Code for a 12-port ADSL LIM. ■ <code>sdsl-atm-v2</code>—Not supported. ■ <code>dadsl-atm-24</code>—Code for a 24-port ADSL LIM. ■ <code>glite-atm-48</code>—Code for an ADSL 48-port G.lite LIM. ■ <code>hdsl2</code>—Code for a 32-port LIM. ■ <code>t1000</code>—Code for T1000 module. ■ <code>ima</code>—Code for a 24-port or 8-port inverse multiplexing over ATM (IMA) T1 or E1 module. ■ <code>stngridsl</code>—Code for an IDSL LIM. ■ <code>40dmt-atm</code>—Code for a 40 channel annex C LIM. ■ <code>48-dmt-atm</code>—Code for a 48 channel annex A LIM. ■ <code>shdsl</code>—Code for an SHDSL LIM. ■ <code>72ct-dmt-atm</code>—Code for a 72 port annex A ADSL LIM. ■ <code>32-dmt-aslam</code>—Not supported. ■ <code>vdsl</code>—Not supported. ■ <code>72-gs-dmt-atm</code>—Not supported.
<code>subtype</code>	Subtype of the image. Following are valid values: ■ <code>normal</code>—Regular image. The default. ■ <code>debug</code>—Debugging image. ■ <code>diagnostic</code>—Diagnostic image.

Command element	Description
source	Location from which the file is loaded. Following are valid values: ■ network host filename—After typing the word network, you can specify a hostname or IP address and path to the file on a TFTP host. ■ console [filename]—The PC connected to the Stinger unit via the serial port. ■ flash device filename—The flash card number and filename of the configuration file. Multiple filenames are allowed for network tar loads.
target-device	Name of the PCMCIA flash card to load. Following are valid device names: ■ [flash-card-] 1 (the default) ■ [flash-card-] 2 The device names can be abbreviated as 1 and 2. You need not specify a target device if the load type is config.

Example To load a configuration file named `unit.cfg` from network host 10.8.7.2 to flash card 1:

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

Example To load Stinger control module image `stngrtcm.ffs` from a TFTP server `pclab-20` and copy the image to the peer control module:

```
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
```

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

```
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
```

Example To load the unitrel.tar file from a network host named host1:

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

Dependencies Consider the following:

- A load operation and a loadmate operation cannot be run simultaneously.
- You can set parameters in the load-select profile to specify which control module images to load to flash memory when you use a load tar command. An explicit load command for a particular module type overrides the settings in the load-select profile. The load command supports type checking to verify that the load type specified on the command line matches the image header.
- If you are using an Asynchronous Transfer Mode (ATM) virtual channel connection (VCC) as an inband management channel, you must be careful when downloading a configuration file using 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 unit 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, to successfully load the configuration proceed as follows:

- a Delete the connection profile and associated atm-qos profile from the configuration file.
- b Load the modified configuration file.
- c 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, no special action is needed.

See Also dircode, format, fsck, load, save

loadmate

Description Loads code images from one control module to the other. The command can be entered from either the primary control module or the secondary control module

Permission level update

Usage loadmate [load-type] [subtype] source-device [target-device]
[filename]

Command element	Description
load-type	Type of image to transfer. If no load type is specified, then all load types that reside on the source device are transferred. Following are valid values: ■ file—Generic file. ■ boot-cm—Control module boot image. ■ cm—Control module image. ■ sds1-atm—Code for an SDSL LIM. ■ al-dmtads1-atm—Code for a 12-port ADSL LIM. ■ sds1-atm-v2—Not supported ■ dads1-atm-24—Code for a 24-port ADSL LIM. ■ glite-atm-48—Not supported. ■ annexb—Not supported. ■ hds12—Not supported. ■ t1000—Not supported. ■ ima—Not supported.
subtype	Subtype of the image. Following are valid values: ■ normal—Regular image (default). ■ debug—Debugging image. ■ diagnostic—Diagnostic image.
source-device	Either of the following: ■ Boot image number (1 or 2) on the source control module for boot images. If no boot number is specified, then boot image 2 is used as the default. ■ PCMCIA flash memory card number of the source control module for nonboot images.
target-device	PCMCIA flash memory card number of the destination control module for nonboot images. This value must be specified for nonboot images, but is not used for boot images.
filename	Name of the file when the load type is file.

Example To copy the control module's software image from 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
```

Example 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
```

Example 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)
```

Dependencies A load and loadmate operation or two loadmate operations cannot be run simultaneously. Both control modules must be running TAOS release 7.11.2 or later.

See Also dircode, format, fsck, load, save

loadslave

Description Loads software to a remote shelf from the host's flash memory. Use of this command is usually optional, because the system performs this function automatically in most cases. For details, see the documentation on hosted operation of remote shelves.

Permission level system

Usage loadslave shelf image

Field	Description
shelf	Specify the shelf ID of the remote shelf.
image	Specify the number of the file to load as shown in the following list:
1	cmb.bin Bootloader image 1.
2	dcmb.bin Bootloader image 2.
3	cm.ffs Operational (runtime) software

Example Before resetting the host, use the loadslave command to transfer the upgraded operational code to each remote shelf. For example, the following commands load the boot code to shelves 2, 3, and 4:

```
HOST> loadslave 2 3
```

```
HOST> loadslave 3 3
```

```
HOST> loadslave 4 3
```

Dependencies This command is functional only within a multishelf configuration. To upgrade the shelves manually, the loadslave command must be entered before resetting the host. (After the reset, system automatically upgrades remote shelves with older software.)

log

Description Specifies that the upper-right or lower-right portion of the status window (or both) must display a message from the Stinger unit's log buffer that contains the most recent system events. If the status window is not already displayed, this command opens it with the connection status information displayed.

The log profile controls whether logs are sent to a syslog host, as well as how many logs are stored in the Stinger unit's buffer. The number of events stored in the log is set by the `save-number` parameter.

Permission level system

Usage log [top | bottom | [-p -r -t]]

Command element	Description
top	Display the log in the upper-right portion of the status window.
bottom	Display the log in the lower-right portion of the status window.
-p	Print the contents of the system log to screen, with the most recent entry first.
-r	Print the contents of the system log in reverse order, with the oldest log entry first
-t	Truncate the command output to the screen width. Many log entries are longer than the standard 80 characters of terminal output. This option truncates the output of the command to the screen width as defined by the current width set by the screen command.
-d	Delete log-entry profiles.

Example To display the system log with the most recent log entry first:

```
admin> log -p
Time      Date      Source                Level  Description
11:11:25  10/16/2002  shelf-1/controller  notice Slot 1/10, state UP 2
11:11:20  10/16/2002  shelf-1/slot-10     info   Software version 9.0.0
11:11:20  10/16/2002  shelf-1/slot-10     info   Card serial number 91469
11:10:15  10/16/2002  shelf-1/controller  notice Slot 1/5, state UP 2
11:10:10  10/16/2002  shelf-1/slot-5       notice 100BaseT: Link down
11:10:10  10/16/2002  shelf-1/slot-5       notice ie1-5-3: Link down
11:10:10  10/16/2002  shelf-1/slot-5       notice ie1-5-2: Link down
11:10:10  10/16/2002  shelf-1/slot-5       notice ie1-5-1: Link down
11:10:10  10/16/2002  shelf-1/slot-5       notice ie1-5-1: Link down
```

To display the event log in the lower portion of the status window:

```
admin> log bottom
```

2 Connections	Status
001 tomw TCP 1/7/14 19200	Serial number: 6201732 Version: 1.0F
002 timl TCP 1/7/3 56000	Rx Pkt: 11185897
	Tx Pkt: 42460
	Col: 129
	12/26/2002 12:20:15 Up: 3 days, 21:47:32
	M: 29 L: info Src: shelf-1/controller
	Issued: 16:48:02, 09/27/2002

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

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 message levels are as follows:

Message level	Description
emergency	A failure or major error has occurred, and normal operation is doubtful.
alert	A failure or major error has occurred, but normal operation can probably continue.
critical	An interface has gone down, or there has been a security error.
error	Something that should not occur has occurred.
warning	Something out of the ordinary, such as a login failure due to an invalid username or password, has happened in otherwise normal operations.
notice	Something of interest, such as a link going up or down, has happened during normal operation.
info	A change in state or status was noticed. Such messages are not of general interest.
debug	The message is of interest only if you are debugging a configuration.

The text of the most recent message is displayed in the middle of the window. You can press the Up-Arrow key to see previous messages, and return to more recent messages by pressing the Down-Arrow key.

Following are some sample informational messages:

Information message	Description
48 out of 48 modems passed POST	All of the modems on a card passed the power-on self test (POST).
Incoming call	A call has been received but not yet routed.
Outgoing call	The unit has dialed a call.
Added Bandwidth	The unit has added bandwidth to an active call.
Ethernet up	The Ethernet interface has been initialized and is running.
LAN session up	A Point-to-Point Protocol (PPP) session has been established.
LAN session down	A PPP session has been terminated.
Assigned to port	The unit has determined the assignment of an incoming call to a digital modem or High-Level Data Link Control (HDLC) channel.
Call Terminated	An active call was disconnected normally, although not necessarily by operator command.
Removed Bandwidth	The unit has removed bandwidth from an active call.
RADIUS config error	The unit has detected an error in the configuration of a RADIUS user profile.
Requested Service Not Authorized	This message appears in the terminal server interface if the user requests a service not authorized by the RADIUS server.

Following are some sample warning messages:

Warning message	Description
Network problem	The call setup was faulty because of problems in the WAN or in the line profile configuration. The D channel might be getting an error message from the switch, or the telephone company might be experiencing a problem.
Call disconnected	The call has ended unexpectedly.
Far end hung up	The remote end terminated the call normally.

Press the Escape key to display a prompt below the status window.

See Also connection, log (profile), view

ls

Description Shows the contents of any PCMCIA flash memory card directory: filename, subtype, status, size, creation date, the amount of space currently in use, and the amount of space available on the card.

Permission level system

Usage ls [socket [/path]]

Command element	Description
socket	Flash card number
/path	Subdirectory on the flash card

Example To list the contents of the flash card on the current control module:

```
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
```

See Also cat, mkdir, mv, rm

M

mkdir

Description Creates a new directory on a PCMCIA flash memory card.

Permission level system

Usage mkdir socket/path

Command element	Description
socket	Flash card number
/path	Subdirectory on the flash card

Example To create the directory test on flash card 1:

```
admin> mkdir 1/test
```

See Also cat, ls, mv, rm

mprt

Description Displays multipath routes.

Permission level system

Usage mprt [-l]

Command element	Description
-l	Display page-by-page output.

Example To list multipath routes page by page:

```
admin> mprt -l
```

MP Route Gateway	Shelf/Slot	IF Addr	Mtu	Switched
1.1.1.1/32				
200.200.200.3	(1/17)	200.200.200.230	1500	0
200.200.200.2	(1/17)	200.200.200.230	1500	0
200.200.200.4	(1/17)	200.200.200.230	1500	0
200.200.200.5	(1/17)	200.200.200.230	1500	0
200.200.200.6	(1/17)	200.200.200.230	1500	0
200.200.200.7	(1/17)	200.200.200.230	1500	0
200.200.200.8	(1/17)	200.200.200.230	1500	0
200.200.200.9	(1/17)	200.200.200.230	1500	0
200.200.200.10	(1/17)	200.200.200.230	1500	0
200.200.200.11	(1/17)	200.200.200.230	1500	0
200.200.200.12	(1/17)	200.200.200.230	1500	0
200.200.200.13	(1/17)	200.200.200.230	1500	0
200.200.200.14	(1/17)	200.200.200.230	1500	0

```

200.200.200.15 ( 1/17)    200.200.200.230  1500  0
200.200.200.16 ( 1/17)    200.200.200.230  1500  0
200.200.200.17 ( 1/17)    200.200.200.230  1500  0
200.200.200.18 ( 1/17)    200.200.200.230  1500  0
200.200.200.19 ( 1/17)    200.200.200.230  1500  0
200.200.200.20 ( 1/17)    200.200.200.230  1500  0
200.200.200.1  ( 1/17)    200.200.200.230  1500  0
200.200.200.21 ( 1/17)    200.200.200.230  1500  0
200.200.200.22 ( 1/17)    200.200.200.230  1500  0

```

mv

Description Moves a file or directory from one file or directory to another on a PCMCIA flash memory card.

Permission level system

Usage mv socket1/path1 socket2/path2

Command element	Description
socket1	Number of the flash card on which path1 is found.
socket2	Number of the flash card on which path2 is found.
path1	File and/or directory to be moved.
path2	File and/or directory that replaces path1.



Note You cannot move a file or directory from one flash card to another with the mv command.

Example To replace the /test1 directory on flash card 1 with the /test2 directory:

```
admin> mv 1/test1 1/test2
```

See Also cat, ls, mkdir, rm

N

netstat

Description Displays the Stinger interface and routing tables, protocol statistics, and active sockets.

Permission level system

Usage netstat [-i] [-g] [-r[host]] [?] [-n | -d] [-s identifiers] [-z]

Command element	Description
No options	Display User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) statistics.
-i	Display the IP interface table.
-g	Display interfaces bound to soft IP addresses.
-r host	Display the IP routing table. You can specify a hostname after the -r option to display the routing table entry for that host.
-?	Display a usage summary.
-n	Display numeric addresses rather than symbolic names (the default).
-d	Display symbolic names rather than numeric addresses.
-s identifiers	Display protocol statistics. If no identifiers follow the -s option, all protocol statistics are printed. If you specify one or more identifiers, they determine the type of protocol statistics to display. Following are the valid protocol identifiers: ■ udp ■ tcp ■ icmp ■ ip ■ igmp ■ mcast
-z	Display zombie routes created for Routing Information Protocol (RIP). Zombie routes are those that have been deleted from the main routing table and are advertised with an infinite metric (16) for a period of 2 minutes to cause neighboring routers to flush this route from their tables.

Example To display both UDP and TCP statistics, do not specify any options:

```
admin> netstat
```

```
udp:
```

-Socket-	Local	Port	InQLen	InQMax	InQDrops	Total Rx
1/c 0		1023	0	1	0	0
1/c 1		route	0	0	0	25
1/c 2		echo	0	32	0	0
1/c 3		ntp	0	32	0	1
1/c 4		1022	0	128	0	0
1/c 5		snmp	0	128	0	0
1/1 0		1	0	256	0	0
1/1 1		1018	0	128	0	0
1/3 0		3	0	256	0	0
1/3 1		1021	0	128	0	0
1/5 0		5	0	256	0	0
1/5 1		1020	0	128	0	0

```
tcp:
```

Socket	Local	Remote	State
1/c 0	*.23	*.*	LISTEN
1/c 1	10.2.3.114.23	15.5.248.121.44581	ESTABLISHED

The display fields contain the following information:

Field	Description
Socket	Shelf, slot, and socket corresponding to a local UDP or TCP port.
Local Port	Port on which the Stinger unit is listening for UDP packets.
InQLen	Number of packets in the input queue for the socket. The packets are waiting to be processed.
InQMax	Maximum number of packets that can reside in the input queue for the socket. A value of 0 (zero) means no limit. The Stinger unit drops excess packets.
InQDrops	Number of packets dropped from the input queue because the value of InQMax was reached.
Total Rx	Total number of packets received on the socket, including dropped packets.
Local	Local IP address and port for a TCP session. For example, in the value 10.2.3.114.23, 10.2.3.114 specifies the IP address and 23 specifies the port for a TCP session. If the address portion contains only an asterisk (*), the Stinger unit is listening for the start of a TCP session.
Remote	Remote IP address and port for a TCP session. For example, in the value 15.5.248.121.44581, 15.5.248.121 specifies the IP address and 44581 specifies the port for a TCP session. If the specification contains only asterisks (*.*), the Stinger unit is listening for the start of a TCP session.

Field	Description
State	State of the session. Following are the possible state values: ■ CLOSED—The socket is not in use. ■ LISTEN—The socket is listening for incoming connections. Note that no session is associated with the LISTEN state, because this state precedes the establishment of a TCP session. ■ SYN_SENT—The socket is trying to establish a connection. ■ SYN_RECEIVED—The connection is being synchronized. ■ ESTABLISHED—The connection is established. ■ CLOSE_WAIT—The remote side has shut down the connection, and the Stinger unit is waiting for the socket to close. ■ FIN_WAIT_1—The socket is closed, and the Stinger unit is shutting down the connection. ■ CLOSING—The socket is closed. The Stinger unit is waiting for acknowledgment that the remote end has shut down. ■ LAST_ACK—The remote end has shut down and closed the socket, and it is waiting for an acknowledgment from the Stinger unit. ■ FIN_WAIT_2—The socket is closed, and the Stinger unit is waiting for the remote end to shut down the connection. ■ TIME_WAIT—The socket is closed, and the Stinger unit is waiting for a remote-shutdown retransmission.

For UDP, netstat reports the following services:

Service	UDP port number
Route	520
Echo	7
NTP	123
SNMP	161
SNMPTrap	162

For TCP, netstat reports the following services:

Service	TCP port number
telnet	23

Example The Stinger interface table shows the address of each interface. To display the Stinger interface table, specify the `-i` option:

```
admin> netstat -i
```

The entries in the interface table associated with the Stinger Ethernet interfaces use the following naming convention, where `ie` stands for interface ethernet:

`ie[shelf] - [slot] - [item]`

For example, the following output shows a four-port Ethernet module in slot 13:

Name	MTU	Net/Dest	Address	Ipkts	Ierr	Opkts	Oerr
ie0	1500	12.65.212.0/24	12.65.212.227	107219	0	54351	0
lo0	1500	127.0.0.1/32	127.0.0.1	4867	0	4867	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
wan4	1500	10.122.99.1	-	0	0	0	0
ie1-12-1	1500	11.168.6.0/24	11.168.6.227	430276	651	0	0
ie1-12-2	1500	10.122.72.0/24	10.122.72.1	0	0	0	3144
ie1-12-3	1500	10.122.73.0/24	10.122.73.1	0	0	3142	0
ie1-12-4	1500	10.122.74.0/24	10.122.74.1		0	0	3141 0

The fields in the interface table contain the following information:

Field	Description
Name	Name of the interface must be one of the following: ■ <code>ie0</code> or <code>ie[shelf] - [slot] - [item]</code>—Indicates an Ethernet interface. ■ <code>lo0</code>—Indicates a loopback interface. ■ <code>rj0</code>—Indicates a reject interface, used in network summarization. ■ <code>bh0</code>—Indicates a blackhole interface, used in network summarization. (Blackhole routes are used to ensure that illegal internet traffic does not pass a firewall.) ■ <code>wanN</code>—Indicates a WAN connection, displayed in this report as it becomes active. ■ <code>wanabe</code>—Indicates an inactive RADIUS dialout profile.
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.

Example To display the routing table, specify the `-r` option. For example:

```
admin> netstat -r
```

Destination	Gateway	IF	Flg	Pref	Metric	Use	Age
0.0.0.0/0	206.65.212.1	ie0	SG	100	1	4891	48630
10.0.0.0/24	11.168.6.249	ie1-12-1	RGT	100	3	0	9236
10.0.100.0/24	11.168.6.86	ie1-12-1	RGT	100	2	0	48601
10.0.200.0/24	11.168.6.86	ie1-12-1	RGT	100	2	0	48601
10.122.72.0/24	-	ie1-12-2	C	0	0	3141	48630
10.122.72.1/32	-	lo0	CP	0	0	0	48630
10.122.73.0/24	-	ie1-12-3	C	0	0	3140	48630
10.122.73.1/32	-	lo0	CP	0	0	0	48630
10.122.74.1/32	-	lo0	CP	0	0	0	48630
10.122.99.0/24	10.122.99.1	wan4	SG	100	7	0	48630
10.122.99.1/32	10.122.99.1	wan4	S	100	7	1	48630
127.0.0.1/32	-	local	CP	0	0	0	48672
127.0.0.2/32	-	rj0	CP	0	0	0	48672
127.0.0.3/32	-	bh0	CP	0	0	0	48672
11.0.2.0/24	11.168.6.249	ie1-12-1	RGT	100	2	0	48626
11.168.6.0/24	-	ie1-12-1	C	0	0	14589	48630
11.168.6.0/24	11.168.6.116	ie1-12-1	*RGIM	100	8	0	48606
11.168.6.0/24	11.168.6.142	ie1-12-1	*RGIM	100	8	0	48610
11.168.6.0/24	11.168.6.96	ie1-12-1	*RGIM	100	8	0	48624

The fields in the routing table contain the following information:

Field	Description
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 field.

Field	Description
IF	Name of the interface through which to send packets over this route: ■ <code>ie0</code> or <code>ie[slot] - [slot] - [item]</code>—Indicates an Ethernet interface. ■ <code>lo0</code>—Indicates a loopback interface. ■ <code>rj0</code>—Indicates a reject interface, used in network summarization. ■ <code>bh0</code>—Indicates a blackhole interface, used in network summarization. (Blackhole routes are used to ensure that illegal internet traffic does not pass a firewall). ■ <code>wanN</code>—Indicates a WAN connection, entered as it becomes active. ■ <code>wanabe</code>—Indicates an inactive RADIUS dialout profile. ■ <code>local</code>—Indicates a single route targeted at the local machine.
Flg	One or more of the following flags: ■ <code>C</code>—A directly connected route, such as Ethernet ■ <code>I</code>—An Internet Control Message Protocol (ICMP) redirect dynamic route ■ <code>N</code>—A route placed in the table via SNMP MIB II ■ <code>R</code>—A route learned from RIP ■ <code>r</code>—A transient RADIUS-like route ■ <code>S</code>—A static route ■ <code>?</code>—A route of unknown origin, which indicates an error ■ <code>G</code>—An indirect route via a gateway ■ <code>P</code>—A private route ■ <code>T</code>—A temporary route ■ <code>M</code>—A multipath route ■ <code>*</code>—A backup static route for a transient RADIUS-like route
Pref	Preference value. See the description of the <code>preference</code> parameter for information about defaults for route preferences.
Metric	RIP-style metric for the route, with a range of 0 through 16.
Use	Number of times the route was referenced since it was created. (Many of these references are internal, so this is not a count of the number of packets sent over this route.)
Age	Age of the route in seconds. RIP and ICMP entries are aged once every 10 seconds.

Example You can include identifiers in the command line to display IP, UDP, TCP, ICMP, and Internet Group Membership Protocol (IGMP) protocol statistics. The system displays TCP statistics collected from line modules as well as the shelf controller. All other types of statistics are collected for the shelf controller only. The following example uses the `tcp` identifier:

```
admin> netstat -s tcp
tcp:
    17 active opens
    160 passive opens
    0 connect attempts failed
    9 connections were reset
    4294967215 connections currently established
    75620 segments received
    82645 segments transmitted
    313 segments retransmitted
    1 active closes
    1 passive closes
```

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

    0 disconnects while awaiting transmission
```

Example The `-g` command option can be used to display the group of connections using the same source-if interface. For example:

```
admin> netstat -g -i sip1
Interface  CONNECTION      remote-address    source address
sip1       pipe1            10.0.0.1          10.0.0.254
sip1       pipe2            10.0.0.2          10.0.0.254
```

You can also include the `all` argument to display groups of connections with source-if configured. The output list is grouped by shared soft IP interface. For example:

```
admin> netstat -g all
Interface  CONNECTION      remote-address    source address
sip1       pipe1            10.0.0.1          10.0.0.254
sip1       pipe2            10.0.0.2          10.0.0.254
sip2       pipe3            15.9.7.1          15.9.7.254
sip2       pipe4            15.9.7.2          15.9.7.254
```

See Also `nslookup`, `ping`, `traceroute`

new

Description Creates an instance of the specified profile type and makes the new profile the working profile. You can also use the command to assign the profile its index value.

To write a new profile, you must uniquely identify it by setting its index field. In a profile listing, a parameter name followed by an asterisk (*) identifies the index field. In most cases, the profile's parameters are assigned default values.

Permission level system

Usage new profile-type [profile-index] [-f]

Command element	Description
profile-type	Type of profile you want to create.
profile-index	Index value of the profile.
-f	Do not prompt for confirmation when issuing a new command that would overwrite the unsaved contents of the edit buffer.

If you create a new indexed profile without using the profile-index argument, a default index (usually null or zero) is used. For example:

Profile type	Default index
user	""
serial	{ any-shelf any-slot 0 }
ethernet	{ any-shelf any-slot 0 }
ip-interface	{ { any-shelf any-slot 0 } 0 }

If you specify the profile-index on the command line, it is validated before use. For example:

```
admin> new sdsl {12 2 3}
error: bad index: unknown value "12"

admin> new system foo
error: profile has no index
```

If you specify a valid index, it is applied to the new profile, which is read into the edit buffer. For example:

```
admin> new sdsl {1 2 3}
SDSL/{ shelf-1 slot-2 3 } read

admin> list
[in SDSL/{ shelf-1 slot-2 3 } (new)]
name=""
physical-address*={ shelf-1 slot-2 3 }
enabled=no
line-config={ 0 0 static { any-shelf any-slot 0 } }
```

Example To create a new connection profile called tim

```
admin> new conn tim
CONNECTION/tim read

admin> list
[in CONNECTION/tim (new)]
station*=tim
active=no
encapsulation-protocol=atm
called-number-type=national
dial-number=""
clid=""
ip-options={ yes yes 0.0.0.0/0 0.0.0.0/0 7 100 255 no no 0 +
session-options={ "" "" no 120 no-idle 120 "" }
telco-options={ ans-and-orig no off 1 no no 56k-restricted 0 +
usrRad-options={ global 0.0.0.0 1646 "" 1 acct-base-10 }
calledNumber=""

admin> write
CONNECTION/tim written
```

Dependencies The index you choose might affect the factory default values set in the profile. For example, if you specify the profile-index default for a user profile, the factory default permission settings are as follows:

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

admin> list
[in USER/default (new)]
name*=default
password=""
active-enabled=yes
allow-termserv=no
allow-system=no
allow-diagnostic=no
allow-update=no
allow-password=no
allow-code=no
allow-debug=no
idle-logout=0
prompt=*
default-status=no
top-status=general-info
bottom-status=log-window
left-status=connection-list
use-scroll-regions=no
log-display-level=none
```

If you specify `admin` instead, the factory-default permissions are set as follows:

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

admin> list
[in USER/admin (new)]
name*=admin
password=MyPW
active-enabled=yes
allow-termserv=yes
allow-system=yes
allow-diagnostic=yes
allow-update=yes
allow-password=no
allow-code=yes
allow-debug=no
idle-logout=0
prompt=*
default-status=no
top-status=general-info
bottom-status=log-window
left-status=connection-list
use-scroll-regions=no
log-display-level=error
```

See Also `delete`, `list`, `read`, `set`, `write`

nslookup

Description Resolves the IP address of a specified hostname by performing a Domain Name System (DNS) lookup. The `ip-global` profile must be configured with the address of at least one DNS server.

Permission level `diagnostic`

Usage `nslookup hostname`

Command element	Description
<code>hostname</code>	The hostname for which you want to obtain an IP address.

Example To look up a host's IP address in DNS:

```
admin> nslookup host-231
Resolving host host-231.
IP address for host host-231 is 10.65.12.231.
```

See Also `netstat`

nvram

Description Provides functions for managing or clearing onboard nonvolatile RAM (NVRAM).

The onboard NVRAM stores the system configuration. Clearing NVRAM initializes the system. If a `default.cfg` is saved to flash memory, the system loads the configuration to NVRAM, which allows minimal configuration. If the system finds no `default.cfg` file, it starts up unconfigured, just as it was when you first installed it. You can then restore the configuration from a recent backup.

Permission level update

Usage `nvram [[[-f] [-r primary_controller | secondary_controller | both_controllers]] [-u|-c|-e|-g|-?]]`

Command element	Description
No options	Clear NVRAM and reset the unit.
-f	Clear NVRAM without prompting for confirmation.
-r	Specify the control module(s) to clear and reboot: ■ <code>primary_controller</code>—Primary control module. ■ <code>secondary_controller</code>—Secondary control module. ■ <code>both_controllers</code> (the default)—Both control modules.
-u	Display NVRAM usage statistics.
-c	Compact the NVRAM storage.
-e	Enable extended profiling.
-g	Generate CDT tree statistic for NVRAM. For internal use only.
-?	Display a usage summary.

Example To display memory usage information:

```
admin> nvram -u
NVRAM seg[0]:start 14000098 size 258040 avail 191680 cmpct 0
```

To clear NVRAM and reset the unit:

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

Dependencies You must reset the Stinger unit after clearing NVRAM and reloading a configuration.

If you add or replace a control module or clear your system configuration, you must enter the `nvram -e` command again from the primary control module to enable extended profiling.

See Also `load`, `reset`, `save`

O

oam

Description Enables you to send F4 and F5 operations, administration and maintenance (OAM) connectivity and loopback testing cells from a port on a Stinger trunk module or line interface module (LIM) to a remote DSL port—for example, to a customer premises equipment (CPE) device.

F4 OAM segment and end-to-end loopback testing is supported only on Stinger trunk modules.

Permission level diagnostic

Usage oam [-e|-c|-l|-p|-L|-C] [slot] [port] [vpi] [vci]

Command element	Description
-e	Display details about the continuity check status.
-c	Run an OAM F5 continuity test.
-l	Run an OAM F5 loopback test.
-p	Turn OAM internal debug on or off.
-L	Run an OAM F4 loopback test.
-C	Run an OAM F4 continuity test.
slot	Slot number.
port	Port number on a CPE device.
vpi	Virtual path identifier (VPI) number.
vci	Virtual channel identifier (VCI) number.
s	Run a segment test. This option must be followed by a value for the n variable.
n	Number of consecutive segments in the segment test.
-q fault loc	Display entries with LOC defects.
-q cc generating	Display OAM entries showing CC cell generation.
-q cc monitoring	Display OAM entries for monitoring CC cells.
-q cc activating	Display OAM entries in the activating state.
-q cc deactivating	Display OAM entries in the deactivating state.

Example To send 64 consecutive segment F4 loopback cells to VPI 15 on DSL port 2, enter the oam command using syntax 2:

```
admin> oam -L 2 15 s 64
```

To display additional information about the outgoing and incoming segment test cells:

```
admin> oam -p
```

To display all active OAM channels:

```
admin> oam -e
OAM Entry list
Entry=826ef120, Linear Port=2003 vpi=0, vci=3 state=Up loopTx=0 loopRx=0
Segment Continuity=READY End2End Continuity=READY isVpc=No
Entry=826ef3b0, Linear Port=2003 vpi=0, vci=4 state=Up loopTx=0 loopRx=0
Segment Continuity=READY End2End Continuity=READY isVpc=No
Entry=826eee50, Linear Port=2003 vpi=0, vci=32 state=Up loopTx=0 loopRx=0
Segment Continuity=READY End2End Continuity=READY isVpc=No
```

```
Total Active Oam Channel=3
```

See Also oamloop

oamloop

Description Sends Asynchronous Transfer Mode (ATM) operation-and-maintenance (OAM) loopback cells on an ATM interface.

Permission level diagnostic

Usage oamloop -e|-s [-c count] [-i sec] shelf slot vpi vci

Command element	Description
-e	(End-to-end). Transmit an end-to-end OAM loop cell, to be looped by the user connection point.
-s	(Segment). Transmit a segment OAM loop cell, to be looped by the first network connection point.
-c count	Transmit the specified number of cells. If this argument is not specified, the count defaults to 0 (zero), which means that the cells are transmitted continuously until the administrator sends an interrupt by pressing Ctrl-C.
-i sec	Transmit the cells at the specified interval in seconds. If this argument is not specified, the interval defaults to 1 second.
shelf	Shelf on which the trunk module is located.
slot	Slot in which the trunk module is located.
vpi	Virtual path identifier (VPI) on which to transmit the looped-back cells.

Command element	Description
vci	Virtual channel identifier (VCI) on which to send the looped-back cells.

Example Following is a sample oamloop command line and output:

```
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
```

See Also oam

open

Description Sets up a telnet-like session across the control bus to a trunk module or line interface module (LIM) so that you can enter commands on that module. Each trunk module and LIM has its own processor, memory, operating system, and set of debug commands.

Permission level diagnostic

Usage open shelf [slot]

Command element	Description
shelf	Shelf ID number. 1 in a Stinger host or standalone unit. 2-7 for a Stinger MRT slave unit. 2-25 for a Stinger Compact Remote slave unit
slot	Number of the expansion slot you want to diagnose (1-16).

Example To open a session with a DS3-ATM trunk module installed in slot 1:

```
admin> open 1 1
```

The prompt changes to show your location, and you can list the available commands:

```
ds3-1/2> ?
```

```
?                ( user )
auth             ( user )
cbcardif         ( debug )
checkd           ( debug )
clear            ( user )
clock-source     ( diagnostic )
debug            ( diagnostic )
debugd           ( debug )
display          ( debug )
dp-ram-display   ( debug )
dpram-test       ( debug )
dspBypassClients ( debug )
dspDial          ( debug )
dspSetDddTimeslot ( debug )
fill             ( debug )
frreset         ( debug )
gdb              ( debug )
help             ( user )
lifDebug         ( debug )
logdebug         ( debug )
logtest         ( debug )
mibcbagt         ( debug )
mibcbreq         ( debug )
mibmgr           ( debug )
modify           ( debug )
nailedState      ( debug )
nlcb             ( debug )
open             ( diagnostic )
quit             ( user )
revision         ( debug )
slots           ( debug )
stackLimit       ( debug )
stackUsage       ( debug )
tdm              ( debug )
timedMsgTest     ( debug )
tprofmgr         ( debug )
tss              ( debug )
update           ( debug )
version          ( system )
whoami           ( user )
```

To return to the control module:

```
ds3-1/2> quit
```

See Also show, slot

ospf

Description Displays information related to Open Shortest Path First (OSPF) routing, including link state advertisements (LSAs), border routers' routing tables, and the OSPF areas, interfaces, statistics, and routing table. You can use the `ospf` command even when OSPF is disabled.

Permission level `system`

Usage `ospf [options]`

The options can be one or more of the following:

Command element	Description
<code>?</code>	Display help information.
<code>size</code>	Display size of the OSPF routing table.
<code>areas</code>	Display OSPF areas.
<code>stats</code>	Display OSPF statistics.
<code>intf [ip_addr]</code>	Display information about one or more OSPF interfaces.
<code>translators</code>	Display the router IDs of not-so-stubby area (NSSA) border routers.
<code>lsa area ls-type ls-id ls-orig</code>	Display detailed information about OSPF LSAs. ■ <code>area</code> is the area ID. ■ <code>ls-type</code> is the LSA type. You can specify one of the following options for <code>ls-type</code>: – <code>rtr</code> (type 1) is a router-LSA that describes the collected states of the router's interfaces. – <code>net</code> (type 2) is network-LSA that describes the set of routers attached to the network. – <code>sum</code> (types 3 and 4) describes routes to networks in remote areas, or autonomous system boundary routers. ■ <code>ls-id</code> is the target address of the router. ■ <code>ls-orig</code> is the address of the advertising router.
<code>lsdb [area]</code>	Display an OSPF link-state database summary for an area. If you do not specify the <code>area</code> option, the summary for the first configured area (or for the only defined area) is displayed. If you specify the <code>area</code> option, the unit displays a summary for the specified area. The <code>area</code> option is meaningful if the unit is operating as an area border router (ABR).
<code>nbrs [ip_addr]</code>	Display information about one or more OSPF neighbors.
<code>routers</code>	Display OSPF router information.
<code>ext</code>	Display OSPF external autonomous system advertisements.

Command element	Description
rtab	Display OSPF routing table.
database ext	Display OSPF database summary.
internal	Display OSPF internal routes.

Example *Displaying the size of the OSPF routing table*

To display information about the size of the OSPF routing table, include the `size` option with the `ospf` command. For example:

```
admin> ospf size
# Router-LSAs:                2
# Network-LSAs:               0
# Summary-LSAs:               0
# Summary Router-LSAs:        0
# AS External-LSAs (type-5):   1
# AS External-LSAs (type-7):   0

# Intra-area routes:          4
# Inter-area routes:           0
# Type 1 external routes:      0
# Type 2 external routes:      0
```

The fields in the output contain the following information:

Field	Specifies
Router-LSAs	Number of router link advertisements known as type 1 LSAs.
Network-LSAs	Number of network link advertisements known as type 2 LSAs.
Summary-LSAs	Number of summary link advertisements known as type 3 LSAs. Type 3 LSAs describe routes to networks.
Summary Router-LSAs	Number of summary link advertisements known as type 4 LSAs. Type 4 LSAs describe routes to autonomous system boundary routers.
AS External-LSAs (type-5)	Number of autonomous system external (ASE) link advertisements known as type 5 LSAs.
AS External-LSAs (type-7)	Number of ASE-7 link advertisements known as type 7 LSAs.
Intra-area routes	Number of routes that have a destination within the area.
Inter-area routes	Number of routes that have a destination outside the area.
Type 1 external routes	Number of external type 1 routes that are typically in the scope of OSPF-IGP.

Field	Specifies
Type 2 external routes	Number of external typ -2 routes that are typically outside the scope of OSPF-IGP.

Example *Displaying 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	Specifies
Area ID	Area number in dotted decimal format.
Authentication	Type of authentication: Simple-passwd, 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 ABRs in the area.
#intnr	Number of reachable internal routers in the area.

Example *Displaying general information about OSPF*

To display general information about OSPF, include the stats option with the ospf command. For example:

```
admin> ospf stats
      OSPF version:          2
      OSPF Router ID:        200.192.192.2
      AS boundary capability: Yes
Attached areas:      1      Estimated # ext.(5) routes:      300
OSPF packets rcvd:  94565  OSPF packets rcvd w/ errs:      0
Transit nodes allocated: 3058  Transit nodes freed:      3056
LS adv. allocated:  1529  LS adv. freed:      1528
Queue headers alloc:  32   Queue headers avail:      32
# Dijkstra runs:      4   Incremental summ. updates:      0
Incremental VL updates:  0   Buffer alloc failures:      0
Multicast pkts sent:  94595  Unicast pkts sent:      5
LS adv. aged out:      0   LS adv. flushed:      0
Incremental ext.(5) updates: 0   Incremental ext.(7) updates: 0
External (type-5) LSA database -
Current state:      Normal
Number of LSAs:      1
Number of overflows: 0
```


The fields in the output contain the following information:

Field	Specifies
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	Yes if the Stinger unit functions as an autonomous system border router (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 ASE-5 routes that the Stinger unit can maintain before it goes into an overload state.
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. allocated	Number of LSAs allocated.
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.
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 unit frees all queue headers from a specific memory block, the Stinger 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.

Field	Specifies
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 ASE-5 updates.
Incremental ext.(7) updates	Number of incremental ASE-7 updates.
Current state	State of the external (type 5) LSA database: Normal or Overload.
Number of LSAs	Number of LSAs in the external (type 5) LSA database.
Number of overflows	Number of ASE-5s that exceeded the limit of the database.

Example *Displaying summarized information about OSPF interfaces*

To display summarized information about OSPF interfaces:

```
admin> ospf intf
```

```
Ifc Address   Phys   Assoc. Area  Type   State   #nbrs #adjs DInt
200.194.194.2 phani  0.0.0.0     P-P    P-P     1     1    120
```

The fields in the output contain the following information:

Field	Specifies
Ifc Address	Address assigned to the Stinger unit's Ethernet interface. To identify WAN links, use the Type and State 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 (Bcast). WAN links are P-P links.
State	State of the link according to RFC 1583. There are many possible states, and not all states apply to all interfaces.
#nbrs	Number of neighbors of the interface.
#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.

Example *Displaying information about a specific OSPF interface*

To display detailed information for a specific interface, use the following syntax:

```
ospf intf ip_addr
```

For example:

```
admin> ospf intf 200.194.194.2
      Interface address:      200.194.194.2
      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:        200.194.194.3
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 adj.:  1
# Mcast floods: 1856 # Mcast acks: 1855
```

The fields in the output contain the following information:

Field	Specifies
Interface Address	IP address of 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 type	Point-to-point (P-P) or broadcast (Bcast).
State	State of the link according to RFC 1583. 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 for the interface.
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.
Rxmt interval	Retransmission interval.
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 networks.

Field	Specifies
Max pkt size	Maximum size of a packet that the Stinger unit can send to the interface.
TOS 0 cost	Type of service (TOS) 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.

Example *Listing the router IDs of NSSA border routers that are translating type 7 LSAs to type 5 LSAs.*

To list the router ID enter the `ospf translators` command. For example:

```
admin> ospf translators
Area ID      Router ID
0.0.0.1      10.105.0.13
0.0.0.2      12.1.1.1
```

Example *Displaying OSPF link state advertisements (LSAs)*

To specify an LSA to be expanded, use the following format 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.

For example, to show an expanded view of an autonomous system external (ASE) LSA for area 0.0.0.0, where the target address of the router is 10.5.2.160 and the address of the advertising router is 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: 0xffffa
      Net mask: 255.255.255.255 Tos 0 metric: 10 E type: 1
      Forwarding Address: 0.0.0.0 Tag: c0000000
```

The fields in the output contain the following information:

Field	Specifies
LSA type	Type of LSA.
ls id	Target address of the router.
adv rtr	Address of the advertising router.
age	Age of the route in seconds.
seq #	Number that begins with 80000000 and increments by one for each LSA received.

Field	Specifies
cksum	Checksum for the LSA.
Net mask	Subnet mask of the LSA.
Tos	Type of service (TOS) for the LSA.
metric	Cost of the link, not of a route. The cost of a route is the sum of all intervening links, including the cost of the connected route.
E type	External type of the LSA indicating either 1 (type 1) or 2 (type 2).
Forwarding Address	Forwarding address of the LSA (described in RFC 1583).
Tag	Tag of the LSA (described in the OSPF RFC).

Example *Displaying an expanded view of a router LSA*

To show an expanded view of a router LSA, use the `rtr` option. For example:

```
admin> ospf lsa 0.0.0.0 rtr 202.1.1.1 202.1.1.1
      LS age:      66
      LS options:  (0x2) E
      LS type:     1
      LS ID (destination): 202.1.1.1
      LS originator: 202.1.1.1
      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 fields in the output contain the following information:

Field	Specifies
LS age	Age of the LSA in seconds.
LS options	Optional functions associated with the LSA. When E is specified, an OSPF area can be configured as a stub area. When T is specified, routes only for type of service (TOS) 0 are calculated.

Field	Specifies
LS type	Type of link as defined in RFC 1583: ■ 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 boundary routers. ■ Type 5 (ASE) are autonomous system external (ASE) LSAs that describe routes to destinations external to the autonomous system. A default route for the autonomous system can also be described by an ASE LSA.
LS ID	IP address of the advertisement's destination.
LS originator	IP address of the advertisement's source.
LS sequence no	Number that begins with 80000000 and increments by one for each LSA. It is used for detecting old and duplicate LSAs.
LS checksum	A checksum covering the entire packet, except for the 64-bit authentication field.
LS length	Length of the LSA in bytes.
Router type	Type of router, either ASBR or ABR.
# router ifcs	Number of interfaces on the router.
Link ID	IP address of the associated router interface.
Link Data	Name of the device on the other side of the link.
Interface type	Type of interface: ■ <code>TransNetwork</code> (transit network)—A network that carries traffic that does not have its source or destination in the network itself. ■ <code>Stub</code> (stub network)—A network in which all external routes are summarized by a default route. ■ <code>P-P</code> (point-to-point)—A link over a serial line.
No. of metrics	Metric for TOS 0.
TOS	Type of service (TOS) for the LSA.
metric	Cost of the link, not of a route. The cost of a route is the sum of all intervening links, including the cost of the connected route.

Example *Displaying an expanded view of a network LSA*

To show an expanded view of a network LSA, include the net option. For example:

```
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)
```

The fields in the output contain the following information:

Field	Specifies
LS age	Age of the LSA in seconds.
LS options	Optional functions associated with the LSA. When E is specified, entire OSPF areas can be configured as stub areas. When T is specified, routes only for TOS 0 are calculated.
LS type	Type of link as defined in RFC 1583: ■ 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 boundary routers. ■ Type 5 (ASE) are autonomous system external (ASE) LSAs that describe routes to destinations external to the autonomous system. A default route for the autonomous system can also be described by an ASE LSA.
LS ID	IP address of the advertisement's destination.
LS originator	IP address of the advertisement's source.
LS sequence no	Number that begins with 80000000 and increments by one for each LSA. It is used for detecting old and duplicate LSAs.
LS checksum	A checksum covering the entire packet, except for the 64-bit authentication field.
LS length	Length of the LSA in bytes.
Network mask	Subnet mask.
Attached Router	Another router running OSPF on the network. The number in parentheses is the cost to that router.

Example *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. For example:

```
admin> ospf lsdb

Area: 0.0.0.0
Type LS ID      LS originator  Seqno      Age  Xsum
RTR  200.192.192.2  200.192.192.2  0x800005f8  696  0x6f0b
RTR  200.192.192.3  200.192.192.3  0x800005f8  163  0x6f09
# advertisements: 2
Checksum total:  0xde14
```

The fields in the output contain the following information:

Field	Specifies
Area	Area ID.
Type	Type of link as defined in RFC 1583: ■ 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 boundary routers. ■ Type 7 are ASE-7 link advertisements that are only flooded within an NSSA.
LS ID	Specifies the target address of the route.
LS originator	Specifies the address of the advertising router.
Seqno	Indicates a hexadecimal number that begins with 80000000 and increments by one for each LSA received.
Age	Specifies the age of the route in seconds.
Xsum	Indicates the checksum of the LSA.
advertisements	Specifies the total number of entries in the link-state database.
Checksum total	Indicates the checksum of the link-state database.

You can expand each entry in the link-state database to view additional information about a particular LSA.

Example *Displaying OSPF neighbor information*

To display information about OSPF neighbors to the Stinger unit, include the `nbrs` options with the `ospf` command. For example:

```
admin> ospf nbrs

Neighbor ID  Neighbor addr  State  LSrxl  DBsum  LSreq  Prio  Ifc
200.192.192.3  200.194.194.3  Full/-  0      0      0      5     phani
```


The fields in the output contain the following information:

Field	Specifies
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.
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.
Prio	Designated router election priority assigned to the Stinger unit.
Ifc	Interface name for the ethernet or connection profile name for the WAN.

To display information about a specific neighbor, include the neighbor's IP address specification with 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
```

The fields in the output contain the following information:

Field	Specifies
OSPF Router ID	IP address of the neighbor.
Neighbor IP address	IP address of the router used to reach the neighbor (often the same address as the neighbor itself).
Neighbor State	State of the link-state database exchange.

Field	Specifies
Physical interface	The name of the interface on which the unit and the neighbor communicate: ■ ie0 or ie[shelf] - [slot] - [item] is an Ethernet interface. ■ wanN is a WAN connection, entered as it becomes active.
DR choice	IP address of the neighbor's designated router.
Backup choice	IP address of the neighbor's backup designated router.
DR Priority	Priority of the designated router.
DB summary qlen	Number of LSAs in the database summary list.
LS rxl qlen	Number of LSAs in the retransmission list.
LS req qlen	Number of LSAs in the request list.
Last hello	How long ago (in seconds) a hello packet was received.
# LS rxmits	Number of link-state update retransmissions.
# Direct acks	Number of direct acknowledgments sent.
# Dup LS rcvd	Number of duplicate LSAs received.
# Old LS rcvd	Number of old link-state updates received.
# Dup acks rcv	Number of duplicate acknowledgments received.
# Nbr losses	Number of times the neighbor went offline.
# Adj. resets	Number of times the adjacency has been re-established after a restart.

Example *Displaying 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) #
ASBR OSPF 200.192.192.3 0.0.0.0 10 200.194.194.3 2
```

The fields in the output contain the following information:

Field	Specifies
DType	Internal route type.
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.

Field	Specifies
#	Number of the interface used to reach the destination.

Example *Displaying OSPF external autonomous system advertisements*

To display OSPF external autonomous system advertisements, include the `ext` option with the `ospf` command. For example:

```
admin> ospf ext
Type LS ID                LS originator    Seqno    Age    Xsum
ASE5 200.192.192.0        200.192.192.2    0x800005f6 751    0xc24d
# advertisements:         1
Checksum total:          0xc24d
```

The fields in the output contain the following information:

Field	Specifies
Type	ASE5.
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 ASE5 database.
Checksum total	Checksum of the ASE5 database.

Example *Displaying the OSPF routing table*

To display the OSPF routing table, include the `rtab` option with the `ospf` command:

```
admin> ospf rtab
DType RType Destination      Area      Cost Flags Next hop(s)  #
RTE  FIX   200.192.192.0/24  -          1   0x82  0.0.0.170    10
RTE  OSPF   200.194.194.2/32  0.0.0.0    20   0x1   200.194.194.3  2
ASBR NONE   200.192.192.2/32  -           0   0x0   None          1
RTE  OSPF   200.192.192.2/32  0.0.0.0     0   0x1   0.0.0.170    10
RTE  OSPF   200.194.194.3/32  0.0.0.0    10   0x101 200.194.194.3  2
RTE  NONE   200.194.194.0/24  -           0   0x2   None          1
ASBR OSPF   200.192.192.3/32  0.0.0.0    10   0x100 200.194.194.3  2
RTE  OSPF   200.192.192.3/32  0.0.0.0    10   0x1   200.194.194.3  2
```

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 (autonomous system border route), or BR (area border route).

Field	Specifies
RType	Internal router type. RType displays one of the following values: FIX (static route), NONE, DEL (deleted), 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.
#	Number of the interface used to reach the destination.

Example *Displaying summarized OSPF database information*

To display summarized information about the OSPF database, include the database option with the ospf command. For example:

```
admin> ospf database
```

```

Router Link States (Area: 0.0.0.0)
Type LS ID      LS originator   Seqno   Age   Xsum
RTR  200.192.192.2  200.192.192.2  0x800005f8  783  0x6f0b
RTR  200.192.192.3  200.192.192.3  0x800005f8  250  0x6f09
      # advertisements:      2
      Checksum total:      0xde14

External ASE5 Link States
Type LS ID      LS originator   Seqno   Age   Xsum
ASE5 200.192.192.0  200.192.192.2  0x800005f6  783  0xc24d
      # advertisements:      1
      Checksum total:      0xc24d
```

If you specify the ext option, the Stinger unit displays only ASE5 LSAs.

The fields in the output contain the following information:

Field	Specifies
Type	Type of link as defined in RFC 1583: ■ 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 boundary routers. ■ Type 5 (ASE) are autonomous system external (ASE) LSAs that describe routes to destinations external to the autonomous system. A default route for the autonomous system can also be described by an ASE LSA. ■ Type 7 are ASE-7 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.

Example *Displaying internal OSPF routes*

When the Stinger unit uses the internal routes feature, it exports routes by means of the router LSA (type 1), instead of by means of the usual ASE-5. If the Stinger unit resides in a stub area and needs to export routes, it cannot use the ASE-5 method. To display internal routes, include the `internal` option with the `ospf` command. For example:

```
admin> ospf internal
Area: 0.0.0.0
Destination  Mask          Cost
10.5.2.160   255.255.255.255  10
10.5.2.161   255.255.255.255  10
100.5.4.78    255.255.255.0    10
```

The fields in the output contain the following information:

Field	Specifies
Area	Name of the area.

Field	Specifies
Destination	Destination of the route.
Mask	Subnet mask for the route.
Cost	Cost of the route.

See Also ospfd

ospfd

Description Displays diagnostic information for Open Shortest Path First (OSPF) tasks.

Permission level system

Usage ospfd [options]

Command element	Description
ospfd adjacency	Display diagnostic information about OSPF adjacency formation.
ospfd all	Display diagnostic information about all OSPF routes.
ospfd debug	Display the current OSPF debug state
ospfd events	Display diagnostic information about OSPF events.
ospfd flood	Display diagnostic information about OSPF flooding.
ospfd lsa	Display diagnostic information about OSPF link-state advertisements (LSAs) that the unit has received and transmitted.
ospfd log	Write debug messages to the log.
ospfd none	Disable the display of all OSPF diagnostic information.
ospfd packets	Display diagnostic information about the current exchange of OSPF packets.
ospfd retransmission	Display diagnostic information about OSPF retransmissions.
ospfd route	Display diagnostic information about the OSPF routing table.
ospfd spf	Display the OSPF algorithm calculations.

Example *Displaying diagnostic information about OSPF adjacency formation*

To display information about OSPF adjacency formation, use the ospfd adjacency command. For example:

```
admin> ospfd adjacency
OSPF-55568: State change, neighbor 8.8.8.2, new state 0x4 (Init),
event 10 (1Way)
OSPF-55568: DR/BDR election begins for iel-34-3
OSPF-55568: Backup Designated Router, changed from 8.8.8.2 to 0.0.0.0
```

```
OSPF-55596: State change, neighbor 8.8.8.2, new state 0x8 (2Way),  
event 3 (2Way)  
OSPF-55596: State change, neighbor 8.8.8.2, new state 0x10 (Exstart),  
event 14 (Go)  
OSPF-55596: DR/BDR election begins for ie1-34-3  
OSPF-55596: Backup Designated Router, changed from 0.0.0.0 to 8.8.8.2  
OSPF-55596: State change, neighbor 8.8.8.2, new state 0x20 (Exchng),  
event 5 (NegDn)
```

Example *Displaying information about current OSPF packet exchanges*

To display information about current OSPF packet exchanges, use the `ospfd packets` command. For example:

```
admin> ospfd packets  
OSPF-254967: Received packet type 1 (Hello) from 10.105.0.2  
(ie1-2-4 ie1-2-4)  
OSPF-54258: Sending multicast, type 5 (LS Ack), destination 224.0.0.5  
(ie1-34-3 ie1-34-3)  
OSPF-54258: Sending unicast type 4 (LS Upd) dst 70.70.70.56
```

Example *Displaying information about all OSPF events occurring on the router*

To display information about all OSPF events occurring on the router, use the `ospfd events` command. For example:

```
admin> ospfd events  
OSPF-54366: State change, neighbor 8.8.8.2, new state 0x1 (Down),  
event 12 (IATim)  
OSPF-54366: DR/BDR election begins for ie1-34-3  
OSPF-54366: Backup Designated Router, changed from 8.8.8.8 to 0.0.0.0
```

Example *Displaying information about the OSPF packets being flooded*

To display information about the OSPF packets being flooded, use the `ospfd flood` command. For example:

```
admin> ospfd flood  
OSPF-254224: From 10.105.0.2, new LS advertisement of age |1|: type 5  
(ASE5) id 22.22.22.22 org 10.105.0.
```

Example *Displaying information by router about LSA generation*

To display information by router about LSA generation, use the `ospfd lsa` command. For example:

```
admin> ospfd lsa  
iproute add 45.45.45.48/32 70.70.70.34  
Route added.  
OSPF-57077: Originating LS advertisement: type 5 (ASE5) id  
45.45.45.48 org 80.80.80.14 of age |0|
```

Example *Displaying information about changes to the routing table*

To display information about changes to the routing table, use the `ospfd route` command. For example:

```
admin> ospfd route
OSPF-255325: Export -> [-] dst=22.22.22.22/32 gw=255.255.255.255 if=-1
cost=16
```

Example *Displaying information about OSPF algorithm calculations*

To display information about OSPF algorithm calculations, use the `ospfd spf` command. For example:

```
admin> ospfd spf
OSPF-255462: Dijkstra calculation performed, on 1 area(s)
OSPF-255462: Destination ASBR 10.105.0.2 now unreachable
```

See Also `ospf`

P

pim

Description `pim` is an administrative system command for displaying information related to protocol independent multicast (PIM) related information.

Permission level `system`

Usage `pim [ groups | rp | nbr | if [ifnum] | bsr | hash [group] ]`

Example The following command displays the bootstrap router (BSR) status immediately after writing the `ip-global` profile:

```
admin> pim bsr
Stinger BSR State : PENDING_BSR
Details of CURRENT BSR:
BSR IP Address      : 0.0.0.0
BSR Interface       : 0
BSR Priority        : 0
BSR holdtime       : 0
BSR Current Frag Tag : 0
BSR HASH masklen    : 0
```

Example The following command shows the static mapping in the group rendezvous point (RP) set for the system:

```
admin> pim rp
Group          RP-Address      RPF neighbor  Priority  holdtime
231.1.1.1/32   1.1.1.3          1.1.1.3      -        -
```

Example The following command shows the PIM neighbor across the Gigabit Ethernet interface:

```
admin> pim nbr
Neighbor      Interface  Priority  Holdtime  DR
1.1.1.10      1          100      105:96    No
```


Example The `pim groups` command displays information about all multicast groups. For example:

```
admin> pim groups
Group Addr  RP/Source Addr upJPTimer  Tree (Rpt/Spt)
223.1.1.1  192.168.101.1  40      RPT
224.4.4.4  10.10.10.10   70      RPT
```

Example The `pim if` command displays information and statistics about the specified PIM interface. For example:

```
admin> pim if 1
pimHelloIntvl      30
pimHelloHoldtime   105
pimHelloPriority    1
pimJpIntvl         60
pimJpHoldtime      210
pimLanPruneDelay   5000
pimOdDelay         2500
pimDR              FALSE
genId              22305411
PIM Statistics
4 packets received
0 bad checksum packets received
0 bad version packets received
3 hello packet received
0 join/prune packets received
0 Boot strap packets received
1 C-RP Adv packets received
5 packets transmitted
4 hello packets sent
0 join/prune packets sent
1 boot strap packets sent
```

Example The `pim hash` command displays the IP address of the best RP for a group or group range. For example:

```
admin> pim hash 234.1.1.1
Best RP for group 234.1.1.1 is 1.1.1.10
```

ping

Description Sends Internet Control Message Protocol (ICMP) Echo Request packets to the specified host as a way to verify that the host is established and the transmission path to the host is open. The host returns ICMP Echo Response packets, and the command generates statistics about the exchange.

Permission level diagnostic

Usage ping [-q|-f host|-v] [-c count] [-i delay] [-s packetsize] hostname

Command element	Description
-q	Quiet. Do not display informational messages. Just display the summary lines at the beginning and end of the command.
-f host	Set the Don't Fragment (DF) bit in the IP header of Ping packets. Setting the DF bit enables the Stinger unit to identify the permissible datagram size, also called the 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 that indicates fragmentation is needed and that the DF bit is set.
-v	Verbose. List every ICMP packet received, except Echo Response packets.
-c count	Send only the specified number of packets.
-i delay	Wait the specified number of seconds before sending the next packet. The default delay period is 1 second.
-s packetsize	Send the specified number of data bytes. The default size is 64 bytes, not including the 8-byte ICMP header. The minimum is 16.
hostname	The station's IP address or Domain Name System (DNS) hostname.

Example To ping a host named Host-231 on a local network:

```
admin> ping host-231
PING host-231 (10.65.12.231): 56 data bytes
64 bytes from 10.65.12.231: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 10.65.12.231: icmp_seq=1 ttl=255 time=0 ms
64 bytes from 10.65.12.231: icmp_seq=2 ttl=255 time=0 ms
64 bytes from 10.65.12.231: icmp_seq=3 ttl=255 time=0 ms
64 bytes from 10.65.12.231: icmp_seq=4 ttl=255 time=0 ms
^C
--- host-231 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max=0/0/0 ms
Press Ctrl-C to stop.
```

Example To exchange only three packets, each of which contains only 16 bytes, use the ping command as follows:

```
admin> ping -c 3 -s 16 host-231
PING host-231 (10.65.12.231): 8 data bytes
16 bytes from 10.65.12.231: icmp_seq=0 ttl=255 time=0 ms
16 bytes from 10.65.12.231: icmp_seq=1 ttl=255 time=0 ms
16 bytes from 10.65.12.231: icmp_seq=2 ttl=255 time=0 ms
--- host-231 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max=0/0/0 ms
```

Example To exchange three packets and suppress the output for each exchange, use the ping command as follows:

```
admin> ping -c3 -q host-231
PING host-231 (10.65.12.231): 56 data bytes
--- host-231 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max=0/0/0 ms
```

See Also netstat, telnet, terminal-server, traceroute

pnnidisplay

Description Displays general information about the Private Network-to-Network Interface (PNNI) implementation, including internal counters.

Permission level system

Usage pnnidisplay

Example Following is sample output that 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
```

The display output contains the following fields:

Field	Indicates
HighestVersion	Highest version of the PNNI protocols supported in the unit.
LowestVersion	Lowest version of the PNNI protocols supported in the unit.
DtlCountOriginator	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 in an entry border node.
CrankbackCount Originator	Number of connection setup messages, including DTL stacks the unit has originated, that have reversed to this node.
CrankbackCountBorder	Number of connection setup messages, including DTL stacks the unit has added in an entry border node, that have reversed to this node.
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 in 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 in 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 because the specified transit network was unreachable or the destination was unreachable.
RteFailUnreachBrdr	Number of times the unit failed to compute a viable partial DTL stack in an entry border node because the target of the path calculation was unreachable. This value indicates those calls that were cleared or cranked back because the specified transit network was unreachable or the destination was unreachable.

See Also pnniinterfacedisplay, pnnilinkdisplay, pnnimapdisplay, pnninnbrdisplay, pnninodedisplay, pnninodetopology, pnniptsestatus, pnnireachableaddr, pnniroutebase.

pnniinterfacedisplay

Description Displays specific interface details for Private Network-to-Network Interface (PNNI).

Permission level system

Usage pnniinterfacedisplay

Example Following is sample command output showing that both ports in trunk module 1 (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

The display output contains the following fields:

Field	Indicates
Port	Dedicated (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 private channels (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 (VBR) service category.
NrtVbr Wt	Configured administrative weight of this interface for the non-real-time 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.

See Also `pnnidisplay`, `pnnilinkdisplay`, `pnnimapdisplay`, `pnninnbrdisplay`, `pnninodedisplay`, `pnninodetopology`, `pnniptsestatus`, `pnnireachableaddr`, `pnniroutebase`.

pnnilinkdisplay

Description Displays information about the operation of logical links attached to the local Private Network-to-Network Interface (PNNI) node and the relationship to nodes on the other end of the links. A PNNI *logical link* is a logical representation of the connectivity between two logical nodes, including the physical link and virtual path connection.

Permission level system

Usage `pnmlinkdisplay [-d [ local node index [ port Id ] ] ]`

Command element	Description
No options	Show a summary of all PNNI logical links.
-d	Show details of all entries.
-d local node index	Show details for the specified local node.
-d local node index port Id	Show details for the specified local node and port.

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					
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					

The display output contains the following fields:

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 }

Field	Indicates
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.
HelloState	State of the Hello protocol exchange across the link or the state of the corresponding LGN Horizontal Link Hello State Machine. 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, 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 upnode has not yet been identified, or if the LinkType is Lowest Level Horizontal Link, the field displays zero.
RemotePortId	Port ID of the port at the other end of the link. If the LinkType field value 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. (<i>Not currently supported.</i>)
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 the neighbor's node ID is not yet known, the field displays zero.
UpnodeAtmAddress	ATM end-system address (AESAs) used to establish connections to the upstream neighbor node. For horizontal links, or when the link type or upstream neighbors node ID is not yet known, the field displays zero.

Example With the `-d` option, the `pnmlinkdisplay` 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.

[illegible]

See Also `pnnidisplay`, `pnniinterfacedisplay`, `pnnimapdisplay`, `pnninnbrdisplay`, `pnninodedisplay`, `pnninodetopology`, `pnniptsestatus`, `pnnireachableaddr`, `pnniroutebase`.

Description Displays information about the Private Network-to-Network Interface (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.

Usage `pnnimapdisplay [-d [local node index [originating node Id
[originating port Id]]]]`

Command element	Description
No options	Display a summary of all Map entries—information about links between local and remote nodes.

-d local node index	Display details of all Map and Metric entries for the specified local node.
-d local node index originating node Id	Display details of all Map and Metric entries for the specified local node and originating node.
-d local node index originating node Id originating port Id	Display details of all Map and Metric entries for the specified local node, the originating node, and the originating port.

Example In the following sample output, the system reports a link on each of its active PNNI ports, with details about the originating and remote port 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
The display output contains the following fields:
```

Field	Indicates
Nd	PNNI node index. Only node index 1 is currently supported.
Index	Which of the many possible maps is referred to. There can be multiple entries for nodal connectivity from a specific node and port pair, in addition to any entry for a horizontal link or uplink (link moving upward in the hierarchy).
OriginatingNodeId	PNNI node ID of the originating node.
OriginatingPortId	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.
RemotePortId	Port ID as assigned by the remote node at the other end of the link from the originating node. If unknown, the field displays zero.

Field	Indicates
MapType	Type of PNNI entity being described by this entry in the map table. Valid values 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 topology state element (PTSE) ID for the PTSE that contains the information group(s) describing the PNNI entity. The PTSE is originated by the originating node.
MetricsTag	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 for the in direction or Out for the out direction).
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.
CLR0	Cell loss ratio for CLP=0 traffic for the service category.
CLR0+1	Cumulative cell loss ratio for CLP=0+1 traffic for the service category.

Example With the -d option, the pnnimapdisplay command displays additional details about each link. In the following example, the command displays information about the link originating on port 802, including the type of link, 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

```

See Also pnnidisplay, pnniinterfacedisplay, pnnilinkdisplay, pnninbrdisplay, pnninodedisplay, pnninodetopology, pnniptsestatus, pnnireachableaddr, pnniroutebase.

pnninbrdisplay

Description Displays information about the relationship between a local Private Network-to-Network Interface (PNNI) node and a neighboring node within the same peer group. A *neighbor node* is a node that is directly connected to a particular node via a logical link.

Permission level system

Usage pnninbrdisplay [-d [local node index [neighbor node Id]]]

Command element	Description
No options	Display a summary of all neighbors—the PNNI node ID and state of its neighbor peers.
-d	Display details of all neighbors.
-d local node index	Display details of all entries for the specified local node.
-d local node index neighbor node Id	Display details of specified local node with the neighbor node.

Example 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
```

The display output contains the following fields:

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 a switched virtual channel connection (SVCC)-based routing control channel (RCC), the field displays zero. (SVCC-based RCCs are currently not supported.)
PeerNodeId	PNNI node ID of the neighboring peer node.
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 PNNI topology state element (PTSE) Request packets received from the neighboring peer.
PeerXmtPtseReq	Number of PTSE Request packets transmitted to the neighboring peer.
PeerRcvPtseAck	Number of PTSE acknowledgement (ACK) packets received from the neighboring peer.
PeerXmtPtseAck	Number of PTSE ACK packets transmitted to the neighboring peer.

Example 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
```

See Also pnnidisplay, pnniinterfacedisplay, pnnilinkdisplay, pnnimapdisplay, pnninodedisplay, pnninodetopology, pnniptsestatus, pnnireachableaddr, pnniroutebase.

pnninodedisplay

Description Displays information about factors that affect the operation of the Private Network-to-Network Interface (PNNI) logical node. Stinger units support a single logical node, which is always a lowest-level node.

Permission level system

Usage pnninodedisplay [-d [local node index]]

Command element	Description
No options	Show a summary of all entries—the node and some state information.
-d	Show details of all entries.
-d local node index	Show details of the specified entry.

Example Following is 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
```

The display output contains the following fields:

Field	Indicates
Node	PNNI node index. Only node index 1 is currently supported.
Node Id	PNNI node ID of the local node.

Field	Indicates
OperStat	Operational status of the node (Up or Down).
DBOverload	Whether the local 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	Level of PNNI hierarchy at which the node exists. Value is from 0 to 104.
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 local node's PNNI routing domain. All lowest-level nodes with the same domain name are presumed to be connected.
AtmAddress	Local node's Asynchronous Transfer Mode (ATM) address.
PeerGroupId	Local node's peer group ID.
RestrictedTransit	Whether the node is restricted to not allowing support of switched virtual circuits (SVCs) (Yes or No).
PglLeaderPri	Leadership priority value the local 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
PglTimeStamp	Time at which the current peer group leader was established.
PreferredPgl	A node that the local node identifies as the leader of its peer group.
PeerGroupLeader	Identifies the current peer group leader.

```
admin> pnninodedisplay -d
```

See Also `pnnidisplay`, `pnniinterfacedisplay`, `pnnilinkdisplay`, `pnnimapdisplay`, `pnninnbrdisplay`, `pnninodetopology`, `pnniptsestatus`, `pnnireachableaddr`, `pnniroutebase`.

Description Displays the information about nodes that the local node has obtained from nodal information Private Network-to-Network Interface (PNNI) topology state element (PTSE).

Usage `pnninodetopology [-d [local node index [node Id]]]`

1-153

Example With no options on the pnninodetopology 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
```

The MapNodeId field is described in the field descriptors table following the next example.

Example 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
    ParentNodeId
    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
    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
    ParentPglNodeId
    00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

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
```


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	Asynchronous Transfer Mode (ATM) address of the node being represented.
RestrictedTransit	Whether the node is restricted to not allowing support of switched virtual connection (SVCs) (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).
OperStat	Operational status of the node (Up or Down).
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).
LeadershipPriority	Leadership priority value the node advertises.
PreferredPgl	A node that the local node identifies as leader of its peer group.
ParentNodeId	If the node is peer group leader, the node ID of the parent logical group node (LGN). If the node is not peer group leader, this field displays zero.
ParentAtmAddress	If the node is peer group leader, the ATM address of the parent LGN. If the node is not peer group leader, this field displays zero.
ParentPeerGroupId	If the node is peer group leader, the node's parent peer group ID. If the node is not peer group leader, this field displays zero.
ParentPglNodeId	If the node is peer group leader, the node ID of the peer group leader of the parent peer group. If the node is not peer group leader, this field displays zero.

See Also pnnidisplay, pnniinterfacedisplay, pnnilinkdisplay, pnnimapdisplay, pnninnbrdisplay, pnninodedisplay, pnniptsestatus, pnnireachableaddr, pnniroutebase.

pnniptsestatus

Description Displays Private Network-to-Network Interface (PNNI) topology state elements (PTSEs) in the local node's topology database.

Permission level system

Usage pnniptsestatus [[originating node Id [ptse type]] | ptse type]

Command element	Description
No options.	Display the current topology database.
originating node Id	Display details of all entries for the specified originating node.
originating node Id ptse type	Display details of all entries for the specified originating node and PTSE type.
ptse type	Display details of all entries for the specified PTSE type. Specify one of following values for the corresponding PTSE types: ■ -o—other ■ -s—nodal state parameters ■ -f—nodal information ■ -i—internal address ■ -e—external address ■ -h—horizontal links ■ -u—uplinks

Example With no options on the command line, the pnniptsestatus command displays the current topology database:

```
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

```

The display output contains the following fields:

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 for the given PTSE as stated in the topology database.
Checksum	The 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.

Example You can specify an originating node ID on the command line, use an option to retrieve information about a specific PTSE type, or 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

```

See Also pnnidisplay, pnniinterfacedisplay, pnnilinkdisplay, pnnimapdisplay, pnninnbrdisplay, pnninodedisplay, pnniptsestatus, pnnireachableaddr, pnniroutebase.

pnnireachableaddr

Description Displays a list of all reachable addresses from each node visible to the local node in the Private Network-to-Network Interface (PNNI).

Permission level system

Usage pnnireachableaddr [-n node Id] | [-a address]

Command element	Description
No options	Display all reachable address entries.
-n node Id	Display for a given node all reachable addresses.
-a address	Display for a given address all entries that match.

Example With no options on the pnnireachableaddr 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
```

Example You can use a `pnnireachableaddr` command option to display reachable addresses from a specified node or Asynchronous Transfer Mode (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
```

The display output contains the following fields:

Field	Indicates
AdvertisingNodeId	PNNI node ID of a node that advertises reachability to the ATM prefix displayed in the <code>ReachableAddr</code> field (displayed in hexadecimal).
PortId	Port ID used by the advertising node to reach the ATM prefix displayed in the <code>ReachableAddr</code> 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 <code>ReachableAddr</code> field.
ReachableAddress	ATM prefix of the reachable address (displayed in hexadecimal).

See Also `pnnidisplay`, `pnniinterfacedisplay`, `pnnilinkdisplay`, `pnnimapdisplay`, `pnnimbrdisplay`, `pnninodedisplay`, `pnninodetopology`, `pnniptsestatus`, `pnniroutebase`.

pnniroutebase

Description Displays the number of current Private Network-to-Network Interface (PNNI) routes from nodes in the PNNI routing domain to valid addresses and transit networks.

Permission level system

Usage `pnniroutebase`

Example `admin> pnniroutebase`
`pnniRouteAddrNumber = 161`

See Also `pnnidisplay`, `pnniinterfacedisplay`, `pnnilinkdisplay`, `pnnimapdisplay`, `pnnimbrdisplay`, `pnninodedisplay`, `pnninodetopology`, `pnniptsestatus`, `pnnireachableaddr`.

pnnisvccrccdisplay

Description The pnnisVccRccDisplay command displays details about switched virtual channel connection (SVCC) based routing control channels (RCCs).

Permission level system

Usage pnnisVccRccDisplay [-d [local node [index]]]

Command element	Description
no options	Display basic information about the SVCC link or links used for RCCs.
-d local node	Display details for all SVCC-based RCCs, or for those associated with a particular local node.

Example To display more details use the -d option. For example, the following output shows details about the SVCC-based RCCs associated with node 1:

```
admin> pnnisvccrccdisplay -d 1
Node Index      Addr:LogItem    VPI|VCI      IntfIndex      HelloState
1      1          {1 17 1}: 0    0 | 32        21          Twoway inside

RemoteNodeId
50:a0:39:84:0f:80:01:bc:72:00:01:17:fd:27:10:ff:1a:80:c3:00:01:01

Version      RcvHellos      XmtHellos
1POINT0      16             16

RemoteNodeId
39:84:0f:80:01:bc:72:00:01:17:fd:27:10:ff:1a:80:c3:00:01:01
```

prtcache

Description Displays statistics about cached RADIUS private-route profiles, and enables you to flush the cache.



Note All cached RADIUS private-route profiles are read-only. You can delete a single cached profile by using the delete command. To delete all cached profiles, use the prtcache command.

Permission level diagnostic, update

Usage prtcache -s [profile_name] | -f [-f] | -t

Command element	Description
-s	Display statistics for all cached private-route profiles.
profile_name	Name of a RADIUS private-route profile. If profile_name is specified, the command displays statistics only for the specified private-route profile.

Command element	Description
-f [-f]	Flush all cached entries. The second -f option specifies that the system flushes all cached routes without waiting for confirmation.
-t	Toggle debug output.

Example To display statistics for all cached private-route profiles:

```
admin> prtcache -s
```

Profile Name	Created	Exp After (min)	Use Count	Refresh Cache
check	12:32:53	1	0	Yes
my-route	10:32:53	23	8	No

The display output contains the following fields:

Field	Description
Profile Name	Name of the cached profile.
Created	Time at which the profile was created.
Exp After	Number of minutes after which the profile is removed from the cache.
Use Count	Number of times the cached profile was referred to in the past.
Refresh Cache	Whether the profile's cache time is refreshed if the profile is used.

Example To display statistics for statistics for the private-route profile named check:

```
admin> prtcache -s check
```

Profile Name	Created	Exp After (min)	Use Count	Refresh Cache
check	12:32:53	1	0	Yes

Example To flush all cached private-route profiles:

```
admin> prtcache -f
```

```
Flush all cached Private Route Table Profiles ? [y/n] y
All cached Private Route Table Profiles flushed.
```

If no profiles have been cached, using the -f option displays the following output:

```
admin> prtcache -f
```

```
Flush all cached Private Route Table Profiles ? [y/n] y
No cached Profiles to flush.
```

If the user does not have the required permission:

```
admin> prtcache -f
```

```
error: Command requires 'diagnose' or 'update' privileges
```

Q

quit

Description Terminates the current telnet session.

Permission level user

Usage quit

Example To terminate the current telnet session:

```
admin> quit
Connection closed by foreign host.
my-station%
```

R

read

Description Reads a copy of the specified profile into the edit buffer, making it the working profile. If the profile is one of a kind, such as the ip-global profile, it has no index field. If an index field exists for a profile, it must be specified on the command line. Only the working profile can be modified. The set and list commands apply only to the working profile.



Note The working profile remains in the edit buffer until you overwrite the buffer with another read command or the new command. To save changes made in the buffer, you must use the write command.

Permission level system

Usage read profile-type [profile-index] [-f]

Command element	Description
profile-type	Type of profile to be read (or the profile itself if it does not require an index specification).
profile-index	Name or address that distinguishes a profile from others of the same type. To see profile indexes, enter the dir command (dir profile-type).
-f	Do not prompt for confirmation when overwriting the unsaved contents of the edit buffer.

By default, if you issue a `read` command that will overwrite the contents of the edit buffer when the buffer contains unsaved changes, the system displays a message prompting for confirmation. For example:

```
admin> read connection david
Reading will overwrite the changes you've made.
Read anyway? [y/n] y
CONNECTION/david read
```

You can avoid this prompt by using the `-f` option on the `read` command line.

Example To find the right index for an `ip-interface` profile, read that profile, and list its contents:

```
admin> dir ip-interface
66 12/20/2002 14:02:02 { { shelf-1 slot-12 1 } 0 }
66 12/27/2002 16:34:40 { { shelf-1 slot-12 2 } 0 }
66 12/27/2002 16:34:47 { { shelf-1 slot-12 3 } 0 }
66 12/27/2002 16:34:54 { { shelf-1 slot-12 4 } 0 }
66 12/28/2002 00:21:06 { { shelf-1 controller 1 } 0 }

admin> read ip-int {{1 c 1} 0}
IP-INTERFACE/{ { shelf-1 controller 1 } 0 } read

admin> list
[in IP-INTERFACE/{ { Shelf-1 controller 1 } 0 }]
interface-address*={ { shelf-1 controller 1 } 0 }
ip-address=10.6.212.227/24
rip-mode=routing-send-and-recv
```

The profile remains in the edit buffer until another `read` command or a `new` command overwrites the buffer. The `set` command modifies the profile. The `write` command saves changes without clearing the buffer.

```
admin> set ip-address=10.6.212.228/24

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

The working profile is represented by a period (.) character. Even after you have used the `get` command to display other profiles, or have entered other commands, you can still use the `get` command to display the working profile:

```
admin> get .
[in IP-INTERFACE/{ { Shelf-1 controller 1 } 0 }]
interface-address*={ { shelf-1 controller 1 } 0 }
ip-address=10.6.212.228/24
rip-mode=routing-send-and-recv
```

See Also `get`, `list`, `new`, `set`, `write`

readflash

Description Displays the contents of `flash-card-1` and `flash-card-2`.

Permission level `update`

Usage `readflash`

Example admin> readflash

```
Flash1 (task "CLI session input task" at 0x80ba2810, time: 71861.25) 64
octets @ 0x80659308
[0000]: a6 0a 0d 00 d6 ec a6 3d 1f 8b 08 00 00 00 00 00
[0010]: 02 03 ec fd 7f 7c 9c 65 95 3f 0e 9f b9 67 26 99
[0020]: a6 d3 f6 4e 3a 4d a7 a5 94 49 72 67 12 da 04 87
[0030]: 12 24 48 90 21 49 a1 2a 6a 5a 42 ad 82 18 d3 02
Flash2 (task "CLI session input task" at 0x80ba2810, time: 71861.25) 64
octets @ 0x80659308
[0000]: a6 0a 0d 00 d6 ec a6 3d 1f 8b 08 00 00 00 00 00
[0010]: 02 03 ec fd 7f 7c 9c 65 95 3f 0e 9f b9 67 26 99
[0020]: a6 d3 f6 4e 3a 4d a7 a5 94 49 72 67 12 da 04 87
[0030]: 12 24 48 90 21 49 a1 2a 6a 5a 42 ad 82 18 d3 02
```

Dependencies The readflash command requires that you enable diagnostic output.

rearslotshow

Description Displays the state of all slots used for line protection modules (LPMs), path selector modules (PSMs), and copper loop test (CLT) modules, and reports the status of the midplane sparing bus.

Permission level System



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. Also, when a copper loop is being tested on a Stinger LS unit with a PSM or CLT module, the command does not display any midplane sparing bus usage.

Usage rearslotshow [shelf]

Command element	Description

shelf	To display the state of all slots used for LPMs, PSMs, and CLT modules, or report the status of the midplane sparing for a remote unit, replace the optional argument shelf with the shelf ID of the remote unit.

Example admin> rearslotshow

Slot	Slot ID
[1]	0 Empty (IRM, LPM)
[2]	0 Empty (IRM, LPM)
[3]	0 Empty (IRM, LPM)
[4]	0 Empty (IRM, 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 ]    0    Empty ( IRM, LPM )
[ 15 ]    0    Empty ( IRM, LPM )
[ 16 ]    0    Empty ( IRM, LPM )
Midplane sparing bus usage :
4          4          3          2          1
8765 4321 0987 6543 2109 8765 4321 0987 6543 2109 8765 4321
.... .... .... .... .... .... .... .... .... ....
```

red-prof-sync

Description Forces the profile context to be transferred from the primary control module to the secondary control module. This command enables you to synchronize the redundant control module profile context at any moment—not just while saving the profile by issuing the `write` command.

Permission level system

Usage red-prof-sync

Example admin> **red-prof-sync**
admin>
Primary Controller: profile transfer to Secondary Controller completed

redundant-controller-switch

Description Enables you to make the secondary control module primary.

If two control modules are available, one of them is the primary controller, and the other one the secondary controller. At start-up time, both controllers negotiate to become primary. You can influence this process by setting the primary preference flag in the `redundancy` profile to the slot number of the controller that will become primary when two controllers are present. If the primary fails, the secondary automatically takes over control of the system. The new primary deactivates all slot modules and reactivates the system.

Permission level system

Usage redundant-controller-switch [-f]

Command element	Description
-f	Forces a switchover.

Example Following are samples of command output under different conditions:

- Command entered on a secondary control module:

```
admin> redundant-controller-switch
This controller is not the PRIMARY, it does not own the bus !
```
- Command entered on the primary control module when the secondary is not requesting to be primary:

```
admin> redundant-controller-switch
The remote controller is not requesting the bus,
it cannot become PRIMARY !
```
- Command entered on the primary control module when no secondary exists:

```
admin> redundant-controller-switch
There is no remote controller !
```

See Also refresh

refresh

Description Opens a connection to a RADIUS server and retrieves the latest configuration information.

Permission level system

Usage refresh -a | -n | -p | -r | -t

Command element	Description
-a	Refresh all types of configuration.
-n	Refresh dedicated (nailed) profile configurations.
-p	Refresh address pool configurations.
-r	Refresh static route configurations.
-t	Refresh terminal server configurations.
-s	Clear the current Source Auth information (purging all existing Source Auth entries from the cache) and reload it from RADIUS.

See Also rad-auth-client

relayoff

Description Turns off an alarm relay.

Permission level diagnostic

Usage relayoff [major | minor]

Command element	Description
major	Turn off the MAJOR relay.
minor	Turn off the MINOR relay.

Example To turn off the MAJOR relay:

```
admin> relayoff major
```

remote

Description Enables you to manage another unit remotely. During a remote management session, the user interface of the remote device is displayed as if you had opened a Telnet connection to the device.

When you use the `remote` command on the shelf controller, the Stinger unit locates the host card that has an active connection to the remote unit. It then opens a session to that card, and uses the `remote` command on the card to bring up the remote management session. The `remote` command uses a proprietary protocol to connect to the remote unit and bring up its user interface.

Permission level diagnostic

Usage remote station_name

Command element	Description
station_name	Specifies the station name of the remote device. The value you enter must match the value of a <code>station</code> parameter in a <code>connection</code> profile, or of the user ID at the start of a <code>RADIUS</code> profile.

Example To manage the unit called `allwyn` remotely:

```
admin> remote allwyn
```

allwynp50 Edit Main Edit Menu Configure >00-000 System 20-000 Ethernet 30-000 Serial WAN	10-100 1 Link A B1 A B2	00-200 11:23:55 MB1 Line Ch Outgoing Call
	20-100 Sessions >1 Active	20-500 DYN Stat Qual Good 01:23:44 OK 1 channel CLUJ 100% ALU 100%
	20-300 WAN Stat >Rx Pkt: 667435 ^ Tx Pkt: 3276757 CRC: 323v	20-400 Ether Stat >Rx Pkt: 99871435 Tx Pkt: 76876757 Col: 73298
	00-100 Sys Option >Security Prof:1 ^ Software +10.0+ S/N:4293801 v	00-400 HW Config >SWAN Interface Adrs: 00c05b45390 Enet I/F: AUJ

Press Ctrl-n to move cursor to the next menu item. Press return to select it.
Press Tab to move to another window--thick border indicates active window.

To exit from the remote management session and return to the command-line interface session on the shelf controller, type Ctrl+C three times in quick succession. Either end of the connection can terminate a Multilink Protocol Plus (MP+) connection by hanging up all channels of the connection.

The Stinger unit generates an error message for any condition that causes the session to terminate before the unit sends the full number of packets. The following messages might appear:

Error message

Explanation

not authorized	Permissions are insufficient for beginning a remote management session. You must authenticate a user profile that enables the system permission.
cannot find profile for station	No profile was found for the specified station name.
profile for station does not specify MPP	A profile was located for the station name, but it did not specify the MP+ encapsulation protocol.
cannot establish connection for station	The MP+ connection to the remote station could not be established.
station did not negotiate MPP	The remote station did not negotiate an MP+ connection.
far end does not support remote management	The remote station is running a version of TAOS that does not support remote management.
management session failed	A temporary condition, such as premature termination of the connection, caused the management session to fail.

Error message

far end rejected session

Explanation

The remote station was configured to reject remote management.

Dependencies Consider the following:

- The connection must use the MP+ protocol.
- The connection must already be established.
- Because your initial permissions are set by the default security profile on the remote system, you might need to authenticate the full access or other administrator-level security profile before managing the unit.
- A remote management session can time out, because the traffic it generates does not restart the idle timer. Therefore, the idle parameter in the connection profile at both the calling and answering ends of the connection must be disabled during a remote management session, and restored just before exiting.
- Remote management works best at higher terminal speeds.

remotesshelf

Description remotesshelf displays information about enabled remote shelves

Permission level system

Usage remotesshelf [-s | -o] Shelf_ID

Command element

Description

With no options

Show information for all remote shelves.

-s

Show detailed information for a single remote shelf.

-o

Show all remote shelves associated with a given OLIM slot.

Example The following command shows details about remote shelf 3:

```
HOST> remotesshelf -s 3
Shelf:          3
Shelf Name:     MyShelfName
Shelf Location: MyShelfLocation
Shelf Type:     Stinger MRT
Host Port:      { { 1 17 1 } 0 }
Shelf Enabled:  Yes
Oper State:     OPER_UP
Up Count:       2
Last Up Time:   Wed Sep 17 15:45:25 2003
Last down Time: Wed Sep 17 15:45:21 2003
```

Example The following command displays all configured remote shelves:

```
HOST> remotesshelf
Shelf Name      AdminState OperState  host-port      up-count
  2 MyShelfName  Enabled   OPER_Down  {{ 0 0 0 } 0 }
```

reset

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

Permission level update

Usage reset [-f] [-m] [-r primary_controller | secondary_controller | both_controllers] [-s shelf_ID]

Command element	Description
-f	Perform the reset without prompting for confirmation.
-m	Reset only the master controller in a hosted system.
-r primary_controller	Reset the primary controller only.
-r secondary_controller	Reset the secondary controller only.
-r both_controllers	Reset both controllers (the default).
-s shelf_ID	Reset a specific remote shelf in a hosted system.

Example With no options, the default action is to reset all controllers in the hosted system:

```
admin> reset
```

See Also nvram

rm

Description Deletes a file or directory on a PCMCIA flash memory card.

Permission level system

Usage rm socket/path

Command element	Description
socket	Flash card number.
path	Subdirectory to be deleted.

Example To remove the /test1 directory on flash card 1:

```
admin> rm 1/test1
```

See Also cat, ls, mkdir, mv

S

save

Description Saves configuration information to a file. The file can reside either on the hard disk of the PC you are using to issue commands to the Stinger unit, or on a networked host. The file is saved in a format that can be loaded into the Stinger unit to restore a configuration.

The `save` command uses the Trivial File Transfer Protocol (TFTP) to transfer the configuration across the network. To save the Stinger configuration on a remote host, you must have the necessary permissions in the directory.

Permission level update

Usage `save [-a] [-m] [-z] [-e encryption_type password]`
`[target [profile-type [profile-index]]`
`| network host filename [-p profile1, profile2...`
`| -x profile1, profile2...]`

Command element	Description
<code>-a</code>	Explicitly save all fields, even those with default values. If you do not specify this option, the file stores only those fields whose values have been changed from the default.
<code>-m</code>	Use Management Information Base (MIB) tags instead of field and value names, and use profile-type numbers rather than profile-type text names.
<code>-z</code>	Save the target configuration files in gzip compressed file format.
<code>-e</code>	Use encryption.
<code>encryption_type</code> <code>password</code>	■ The <code>encryption_type</code> argument specifies the method to be used for encryption and decryption. You can specify DES or MD5. ■ The <code>password</code> argument specifies the password used to generate the key for encryption and decryption. ■ The <code>-e</code> option supports only a network target.
<code>target</code>	Destination of the file to be saved. Valid specifications are: ■ <code>network host filename</code>—A network hostname or IP address and the name of the file on that host. ■ <code>console</code>—The PC you are using in a terminal session. ■ <code>flash device filename</code>—The PCMCIA flash memory card.

Command element	Description
profile-type	Type of profile to be read, or the profile itself if it does not require an index specification.
profile-index	Name or address that distinguishes a profile from others of the same type. To see profile indexes, enter the <code>dir profile-type</code> command.
network host filename	Hostname or IP address of the source network and the name of the file on that host.
-p profile1, profile2...	Save the specified list of profiles (used only with the network option).
-x profile1, profile2...	Save all profiles, except those in the specified list (used only with the network option).



Note Most telnet utilities have a capture function. For example, `telnet.cfg` has a capture function under the file menu. Start the capture before issuing the `save` command, and end the capture after the terminal display has ended. The capture function usually reports the name of the target file into which the display has been saved.

Example To save all connection profiles to a file on a PC's hard disk (after starting the capture utility in the terminal emulation software):

```
admin> save console connection
; saving profiles of type CONNECTION
; profile saved Thu Jan 2 13:02:54 2002
new CONNECTION dallas
set active=yes
set ip-options remote-address=10.122.99.1/24
write -f
;
; profile saved Thu Jan 2 13:02:54 2002
new CONNECTION chicago
set active=yes
set dial-number=999
set ip-options remote-address=10.168.6.57/24
set ip-options routing-metric=2
write -f
;
```

To save the file, stop the capture in the terminal emulation software.

Example To save the entire configuration to hard disk, start the capture utility and specify the console option:

```
admin> save console
; saving all profiles
...
```

All configured profiles and parameters scroll to the capture buffer. When the entire configuration has been displayed, the following output appears:

```
;
;
; all profiles saved
```

To save the file, stop the capture.

Example The following example shows how to save a specific profile to a file on a network host:

```
admin> save network host-231 /users/marcel/ipglobal ip-global
configuration being saved to 10.65.12.231
file /users/marcel/ipglobal...save
admin>
```

Example The following example shows how the save command specifies a profile type by its internal number when saving with the -m option:

```
admin> save -m console system
; saving profiles of type SYSTEM
; profile saved Sat Mar 29 13:29:42 2002
new 3
set 1=1
set 2=eng-lab-43
write -f
```



Note If the first item following a new, read, or dir command is numeric, the system handles the item as a profile-type number.

See Also load, nvram

screen

Description Changes window display sizes for the current session only. If the status window is open when you enter the screen command, the window is resized dynamically. If it is not open, the status window is resized when you next open it.

Permission level update

Usage screen [screen-length] [status-length] [-w width]

Command element	Description
screen-length	Number of lines displayed in the command-line window. The default is 24 lines, which is the minimum size. The maximum size is 999 lines

Command element	Description
status-length	Number of lines displayed in the status window, including dividing lines. The default is 18 lines, which is the minimum size. The maximum size is 993 lines. The status-length value must be less than screen-length by at least 6 lines
-w width	Screen width, a value from 80 (the default) to 256.

Example If only the screen-length argument is specified, and the stored status-length is not less than the specified value by six lines, the status-length is automatically adjusted. This scenario is demonstrated in the following example:

```
admin> screen 55 22
new screen-length 55
new status-length 22

admin> screen 24
error: screen-length conflict, adjusting status-length from 22 to 18
new screen-length 24
new status-length 18
```

Example The screen command enables you to specify the width of the screen. For example, the following command sets the screen width to 256 characters:

```
admin> screen -w 256
```

The specified screen width is the number of characters that are visible without scrolling, including the system prompt and spaces following it.

For example, if the screen width is 80 characters and the prompt is admin> (a 6-character prompt followed by a space), the maximum number of visible characters in a command is 72. If you enter a long command (for example, one that has 100 characters), 28 of the characters are not visible at any one time. You can scroll to the characters not currently visible by moving the cursor left or right. The Ctrl-L, Ctrl-R control sequence allows you to redraw the current line.

See Also screen-length, screen-width

sdslines

Description Displays SDSL channel information.

Permission level system

Usage sdslines -a | -d | -f | -sh | -sl | -u

Command element	Description
-a	Display all available channels.
-d	Display all disabled channels.
-f	Display all possible channels.
-sh shelf	Limit the output to lines on the specified shelf.

Command element	Description
-sl shelf slot	Limit the output to lines on the specified slot.
-u	Display all in-use channels.

Example To display all SDSL channels available, use the -a option:

```
admin> sdsllines -a
```

All SDSL lines:

			(dvOp	dvUpSt	dvRq	sAdm	na1lg)
Line	{	1 3 1 }	(Up	Idle	UP	UP	00001)
Line	{	1 3 2 }	(Up	Assigned	UP	UP	00002)
Line	{	1 3 3 }	(Up	Assigned	UP	UP	00003)
Line	{	1 3 4 }	(Up	Idle	UP	UP	00004)
Line	{	1 3 5 }	(Up	Idle	UP	UP	00005)
Line	{	1 3 6 }	(Up	Assigned	UP	UP	00006)
Line	{	1 3 7 }	(Up	Idle	UP	UP	00007)
Line	{	1 3 8 }	(Up	Assigned	UP	UP	00008)
Line	{	1 3 9 }	(Up	Assigned	UP	UP	00009)
Line	{	1 3 10 }	(Up	Assigned	UP	UP	00010)
Line	{	1 3 11 }	(Up	Assigned	UP	UP	00011)
Line	{	1 3 12 }	(Up	Assigned	UP	UP	00012)
Line	{	1 3 13 }	(Up	Assigned	UP	UP	00013)
Line	{	1 3 14 }	(Up	Assigned	UP	UP	00014)
Line	{	1 3 15 }	(Up	Assigned	UP	UP	00015)
Line	{	1 3 16 }	(Up	Idle	UP	UP	00016)

The data displayed includes the physical address and channel number, and the following status information about each channel:

Field	Description
dvOp	The current operational state of the channel (also specified by the device-state parameter): - Down—Indicates that the channel is in a nonoperational state. - Up—Indicates that the channel is in normal operations mode.
dvUpSt	The status of the channel in normal operations mode: - Idle—Indicates that no call is on the line. - Active—Indicates that the channel is handling a call.
dvRq	The required state of the channel as specified by the reqd-state setting: - Down—Indicates that the channel is required to be nonoperational. - Up—Indicates that the channel is required to be in normal operations mode.

Field	Description
sAdm	The desired administrative state of the line: ■ Down—Indicates that the line should terminate all operations and enter the down state. ■ Up—Indicates that the line should start up in normal operations mode. The 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 that should change the Stinger unit to the state desired.
nailg	The dedicated (nailed) group to which the line is assigned.

See Also device-type, device-state

set

Description Sets a parameter’s value or displays help text for a parameter in the current or specified context of the working profile. To save the new setting, you must write the profile.

Permission level system

Usage set param-name [param-index] [subprofile] = value | ?

Command element	Description
param-name	Name of the parameter in the current or specified context of the working profile.
param-index	Parameter index, which might be required for complex parameters. (See the physical-address parameter example.)
subprofile	Subprofile name within the working profile. By specifying its name on the command line, you can set a parameter in a subprofile without opening the subprofile.
= value	Valid parameter value. The equals (=) sign is part of the required syntax unless you are using the question mark (?) for help.
?	Display help text about the specified parameter. Omit the equals (=) sign. To display help about the address parameter, for example, enter set address ? from within the profile and subprofile that contains the address parameter.

Example set enabled = yes

See Also list, new, physical-address, read, write

shdslines

Description Displays the status of all SHDSL lines.

Permission level system

Usage shdslines [-a | -d | -f | -u | -sh | -sl | -t]

Command element	Description
-a	Show all SHDSL lines.
-d	Show disabled lines
-f	Show all free lines
-u	Show in-use lines
-sh shelf	Limit the output to lines on the specified shelf.
-sl shelf slot	Limit the output to lines on the specified slot.
-t	Toggle debug flag.

Example To show all free lines:

admin> shdslines -f

Free SHDSL lines:

					(dvOp	dvUpSt	dvRq	sAdm	nailg)	
Line	{	1	4	3	}	(Down	Idle	UP	UP	00153)
Line	{	1	4	4	}	(Up	Idle	UP	UP	00154)

The data displayed includes the physical address of each line and the following status information:

Field	Description
dvOp	The 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	The 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	The 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 operations mode.

Field	Description
sAdm	The desired administrative state of the line: ■ Down specifies that the line should terminate all operations and enter the deactivated state. ■ Up specifies that the line should be activated in normal operations mode. The 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 (for example, someone has dialed in) that should change the Stinger unit to the desired state.
naileg	The dedicated (nailed) group to which the line is assigned.

show

Description Displays information about installed modules and their status.

Permission level system

Usage show [-a ... | -s [shelf-number [slot-number [item-number]]]

Command element	Description
No options	List all modules in the system.
-a ...	Include modules absent. Display all slots that the Stinger unit currently maintains state information for, including slots in the state of none. The none state indicates that configuration profiles are being preserved for a slot whose module has been removed.
-s	Show additional information for debugging.
shelf-number	The shelf ID number. 1 in a Stinger host or standalone unit. 2-7 for a Stinger MRT slave unit. 2-25 for a Stinger Compact Remote slave unit
slot-number	The slot number. (1-16)
item-number	The item number.

Example To display all installed modules:

```
admin> show
Shelf 1 ( master ):

                Req'd  Oper  Slot Type
{ 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    ds3-atm-trunk-daughter-card
{ shelf-3 slot-1 0 }    UP    UP    mrt-36-adsl-card
{ shelf-3 first-control-mod+ UP    UP    mrt-cm
```

The output includes the address of each slot in which an expansion module is installed, the required status and actual operating status of the module, and the type of module installed. The required and operating status can be one of the following:

Status	Description
UP	Normal operational mode. The module is activated and running.
DOWN	Not in an operational mode. The module has shut down all functions and can be deactivated by the shelf controller.
POST	The download is complete, and the devices in the module are running power-on self tests (POSTs).
BOOT	The module is running BOOT code. Under normal conditions, the LOAD status follows.
LOAD	The module is loading code as part of starting up.
RESET	The module is being reset.
NONE	The module has been swapped out, but its configuration remains in flash memory.
OCCUPIED	The module is using two slots.
DIAG	The specified remote shelf coredumps across the host system and does not have a local Ethernet interface.

See Also device, slot

sleep

Description Specifies the number of seconds the system pauses before it executes the next command.

Permission level system

Usage sleep [seconds]

Command element	Description
seconds	A value from 0 through 60 seconds. The default setting is 5 seconds.

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

```
admin> sleep 10
```

The `sleep` command is useful for provisioning connection profiles using the NavisAccess™ management software. The command enables the system to completely delete an old configuration profile before using a new profile with the same name. NavisAccess™ management software users can introduce this command in a configuration file sent to a Stinger unit to time saving the configuration profiles.

slot

Description Changes the administrative state of a module, forcing a state change (up or down). The down state allows temporary removal of a card without the loss of its configuration.

Permission level diagnostic

Usage `slot -u | -d | -r | -t | -b | -m | -w [shelf-number [slot-number]]`

Command element	Description
<code>-u</code>	Activate the specified module.
<code>-d</code>	Deactivate the specified module.
<code>-r</code>	Delete the profiles for a module that has been removed.
<code>-t</code>	Toggle module debug level.
<code>-b</code>	Force a hardware reset of a module.
<code>-m</code>	Put a module into maintenance state.
<code>-w</code>	Change or display the watchdog failure limit.
<code>shelf-number</code>	Shelf ID number. 1 in a Stinger host or standalone unit. 2-7 for a Stinger MRT slave unit. 2-25 for a Stinger Compact Remote slave unit
<code>slot-number</code>	Number of an expansion slot in the specified shelf (1 through 16).

The Stinger unit generates new syslog records when you use the following commands:

- `slot -b`—Reset a module.
- `slot -d`—Stop operation of a module.
- `slot -u`—Start operation of a module.

When you use `slot -b` or `slot -d`, the Stinger unit also generates new nonvolatile RAM (NVRAM) records.

Example To start up the expansion module in slot 5:

```
admin> slot -u 5
slot 1/5 state change forced
```

Example In the next example, a module has been removed, as indicated by a status of **NONE** in the output of the **show** command:

```
admin> show 1 4
Shelf 1 ( standalone ):
  { shelf-1 slot-4 0 }      UP      al-dmtadsl-atm-card:
  { shelf-1 slot-4 1 }      UP      xdsl-12-line1
  { shelf-1 slot-4 2 }      UP      xdsl-12-line-2
  { shelf-1 slot-4 3 }      UP      xdsl-12-line-3
  { shelf-1 slot-4 4 }      UP      xdsl-12-line-4
  { shelf-1 slot-4 5 }      UP      xdsl-12-line-5
  { shelf-1 slot-4 6 }      UP      xdsl-12-line-6
  { shelf-1 slot-4 7 }      UP      xdsl-12-line-7
  { shelf-1 slot-4 8 }      UP      xdsl-12-line-8
  { shelf-1 slot-4 9 }      UP      xdsl-12-line-9
  { shelf-1 slot-4 10 }     UP      xdsl-12-line-10
  { shelf-1 slot-4 11 }     UP      xdsl-12-line-11
  { shelf-1 slot-4 12 }     NONE     xdsl-12-line-12
  { shelf-1 slot-4 13 }     UP      xdsl-12-virt-device
```

The **NONE** status indicates that the module was removed but that its profiles have been saved. The Stinger unit retains information about the module that was in the slot and saves its profiles until a module of a different type is installed in the same slot, or until you delete the profile:

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

Either action deletes all the old profiles associated with the slot. When you insert a different type of module, the system creates appropriate new profiles.



Note If you replace a line interface module (LIM) and wish to retain the existing Asynchronous Transfer Mode (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. A soft permanent virtual circuit (SPVC) initiator switch can reestablish subscriber SPVCs, because the SPVC addresses have not changed.

See Also `device`, `open`, `show`

slot-clock-source

Description Shows the clock sources available from trunk modules.

Permission level diagnostic

Usage `slot-clock-source`

Example To show the available clock sources:

```
admin> slot-clock-source
```

```
Best line: 18.1
```

```
Local Source List:
```

```
Source: line 18.1 Available*    priority: 2
```

The clock source is displayed in `slot.line` format, in which `slot` indicates the trunk module slot number and `.line` indicates the trunk module line number.

snmpauthpass

Description Generates the authentication key of a Simple Network Management Protocol version 3 (SNMPv3) user-based security model (USM) user.

Permission level update

Usage `snmpauthpass username password`

Command element	Description
<code>username</code>	SNMPv3 USM user for whom an authentication key is generated.
<code>password</code>	Password for generating the authentication key.

The `snmpauthpass` command can accept a username in escape sequence format.

Example To generate the authentication key of the user `robin` with the password `abc123`:

```
admin> snmpauthpass robin abc123
```

Dependencies 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.

See Also `snmpprivpass`

snmpprivpass

Description Generates the privacy key of a Simple Network Management Protocol version 3 (SNMPv3) user-based security model (USM) user.

Permission level update

Usage `snmpprivpass username password`

Command element	Description
<code>username</code>	SNMPv3 USM user for whom a privacy key is generated.
<code>password</code>	Password for generating the privacy key.

The `snmpprivpass` command can accept a username in escape sequence format.

Example To generate the privacy key of the user `robin` with the password `abc123`:

```
admin> snmpprivpass robin abc123
```

Dependencies 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.

sntp

Description Displays statistics concerning the state of the Simple Network Time Protocol (SNTP) server.

SNTP enables a group of servers to synchronize their clocks with reference to a primary time server. The SNTP server retrieves the correct time from an official source and distributes the information to other servers and networks.

Permission level system

Usage `sntp -d`

Example `admin> sntp -d`

```
SNTP:
mode: disabled, threshold: 10
max delta: 0, last Delta: 0
waiting for first update
system start time: Wed Oct 11 15:18:40 2000
original system start time: Wed Oct 11 15:18:40 2000
SNMP start delta: 5
SNMP trap sent: 0
time left for next request: 0 sec
```

splimports

Description Displays the redundancy or ignore-lineup setting for a line interface module's (LIM) ports.

Permission level debug

Usage `splimports -i [ -n | -s | -y ] | -s [ -a | -i | -m | -w ] [slotnumber]`

Command element	Description
<code>-i</code>	Ignore-lineup feature setting for LIM ports. Use the <code>-i</code> option with the following arguments to display specific ignore-lineup settings: <code>-n</code>—Ports that are disabled for the ignore-lineup feature. <code>-s</code>—Ports that are configured for system-defined ignore-lineup.

Command element	Description
	-y—Ports that are enabled for the ignore-lineup feature (default option).
-s	Redundancy setting for LIM ports. Use the -s option with the following arguments to display ports with specific redundancy settings: -a—Ports enabled for automatic redundancy. -i—Ports that are disabled for automatic or manual redundancy. -m—Ports enabled for manual redundancy. -w—Ports enabled for both automatic and manual redundancy (default option).
slotnumber	Settings for ports in the specified slot. If no slot number is specified, the command applies to all slots.

```
Example admin> splimports -i -s
Line      Type
-----
1-1-1     SDSL
1-1-2     SDSL
1-1-3     SDSL
1-1-4     SDSL
1-1-5     SDSL

admin> splimports -s -i
Line      Type      Sparing Mode
-----
1-1-1     SDSL      Inactive
1-1-2     SDSL      Inactive
1-1-3     SDSL      Inactive
1-1-4     SDSL      Inactive
1-1-5     SDSL      Inactive
```

spvcc

Description Displays Asynchronous Transfer Mode (ATM) soft permanent virtual channel connection (PVCC) statistics.

Permission level system

Usage spvcc [-a | -sh | -s | -p | -d] shelf slot port vpi

Command element	Description
-a	Show all ATM soft PVCC entries.
-sh shelf	Show ATM soft PVCC entries by shelf.
-s shelf slot	Show ATM soft PVCC entries by slot.
-p shelf slot port	Show ATM soft PVCC entries by slot and port.
-d shelf slot port vpi	Show detailed information about an ATM soft PVCC associated with a specific virtual path identifier (VPI).

Example To display detailed statistics for a specific PVCC, you can first show all ATM soft PVCCs to verify the slot, port, and VPI of the one you want. Then, enter the spvcc command again with that information:

```
admin> spvcc -a
Profile Intf/Slot/Port/ VPI/ VCI/targVPI/targVCI TargSel OStatus
spvc1  16  1  2  0  32  0      33      req  inProg
.....
admin> spvcc -d 16 2 0
Profile = ray-1
Physical Address = { 1 1 2 }
Interface = 16
OperStatus = inProg
VCL Vpi = 0
VCL Vci = 32
TargetSelect = req
TargetVpi = 0
TargetVci = 33
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 = 19
RetryInterval = 10
RetryTimer = 7
RetryThreshold = 1
RetryLimit = 0
```

spvcshow

Description Shows Asynchronous Transfer Mode (ATM) soft permanent virtual circuit (SPVC) addresses.

Permission level system

Usage spvcshow [-a | -sh | -s | -p] shelf slot port

Command element	Description
-a	Show all ATM SPVC addresses.
-sh shelf	Show ATM SPVC address entries by shelf.
-s shelf slot	Show ATM SPVC address entries by slot.
-p shelf slot port	Show ATM SPVC address entries by slot and port.

Example To show the ATM SPVC addresses for all ports on remote shelf 2:

```
admin> spvcshow -sh 2
ADDR:Item Stat SPVC-ATM-Address
2-1-1:0 up 39:84:0f:80:01:bc:72:00:01:0d:61:c0:39:ff:00:00:00:01:01:00
2-1-2:0 down 39:84:0f:80:01:bc:72:00:01:0d:61:c0:39:ff:00:00:00:01:02:00
2-1-3:0 down 39:84:0f:80:01:bc:72:00:01:0d:61:c0:39:ff:00:00:00:01:03:00
2-1-4:0 down 39:84:0f:80:01:bc:72:00:01:0d:61:c0:39:ff:00:00:00:01:04:00
2-1-5:0 up 39:84:0f:80:01:bc:72:00:01:0d:61:c0:39:ff:00:00:00:01:05:00
2-1-6:0 down 39:84:0f:80:01:bc:72:00:01:0d:61:c0:39:ff:00:00:00:01:06:00
2-1-7:0 down 39:84:0f:80:01:bc:72:00:01:0d:61:c0:39:ff:00:00:00:01:07:00
2-1-8:0 up 39:84:0f:80:01:bc:72:00:01:0d:61:c0:39:ff:00:00:00:01:08:00
2-1-9:0 up 39:84:0f:80:01:bc:72:00:01:0d:61:c0:39:ff:00:00:00:01:09:00
2-1-10:0 down 39:84:0f:80:01:bc:72:00:01:0d:61:c0:39:ff:00:00:00:01:0a:00
2-1-11:0 down 39:84:0f:80:01:bc:72:00:01:0d:61:c0:39:ff:00:00:00:01:0b:00
2-1-12:0 down 39:84:0f:80:01:bc:72:00:01:0d:61:c0:39:ff:00:00:00:01:0c:00
...
```

See Also spvcc, spvpc

spvcstat

Description Show overall Asynchronous Transfer Mode (ATM) soft permanent virtual circuit (SPVC) and soft permanent virtual path (SPVP) information.

Permission level system

Usage spvcstat

Example admin> spvcstat

```
Call Failures = 88
Currently Failing PVCCs = 1
Currently Failing PVPCs = 1
```

spvpc

Description Displays Asynchronous Transfer Mode (ATM) soft permanent virtual path connection (PVPC) statistics.

Permission level system

Usage spvpc [-a | -sh | -s | -p | -d] shelf slot port vpi

Command element	Description
-a	Show all ATM soft PVPC entries.
-sh shelf	Show ATM soft PVPC entries by shelf.
-s shelf slot	Show ATM soft PVPC entries by slot.
-p shelf slot port	Show ATM soft PVPC entries by slot and port.
-d shelf slot port vpi	Show detailed ATM soft PVPC information.

Example To display detailed statistics for a specific PVPC, you can first show all ATM soft PVPCs to verify the shelf, slot, port, and VPI of the one you want. Then enter the spvpc command again with that information:

```
admin> spvpc -a
Profile      Shelf/Slot/Port  VPI/targVPI  TargSel  OStatus  RFail  LastCause
spvp-2.1     1    2    1    15  15      req    inProg  21  RecOnTimerExpiry
....
admin> spvpc -d 1 18 2 5
Profile = spvc-init-1
Physical Address = { 1 18 2 }
OperStatus = inProg
VCL Vpi = 5
TargetSelect = req
TargetVpi = 0
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
```

stats

Description Collect and display AAL5, ATM, or Ethernet statistics for the specified port or device.

Permission level system

Usage stats stats-cmd [np] stats-type [port|conn-id|all]

Command element	Description
stats-cmd	One of the following actions: ■ enable—Enable statistics collection on the specified port or device. ■ disable—Disable statistics collection on the specified port or device. ■ traffic—Display traffic statistics. ■ rate—Display traffic statistics per second. This command toggles the display of rate information. ■ error—Display error statistics. ■ clear—Clears statistics.
stats-type	Type of statistics to report. Specify one of the following values: ■ aal5—AAL5 statistics for Fast Ethernet Trunk module. ■ atm—ATM statistics on the Utopia port for the Fast Ethernet Trunk module. ■ ether—Statistics for the Fast Ethernet Trunk module's Ethernet ports.

Command element	Description
<code>np stats-type</code>	Type of information to display about network processor operations. Specify one of the following options: ■ <code>app</code>—APP driver statistics. ■ <code>conn slot ifnum</code>—Connection statistics. Optional arguments are: – <code>slot</code>—Display statistics only for the specified slot. – <code>slot ifnumber</code>—Display statistics only for the specified interface. You must also specify a slot number. ■ <code>fpp</code>—Fast Pattern Processor (FPP) statistics. FPP is a component of the network processor. ■ <code>ipqos ifnum [up down]</code>—IP QoS statistics. For VLAN circuit or stacked VLAN connections, replace <code>ifnum</code> with the WAN interface number. For VLAN circuit or stacked VLAN connections, you must also specify the direction in which the traffic flow is to be monitored. To monitor upstream traffic transmitted over an interface, specify <code>up</code>; specify <code>down</code> to monitor downstream traffic. The <code>up</code> and <code>down</code> options are not applicable to routed and transparent-bridged connections. ■ <code>lport lportnum [count count rspslot]</code>—Logical port statistics. <code>lportNum</code> is the logical port number, a value from 1 through 16. <code>count</code> specifies the number of entries to display. Valid values are from 1 through 16. If you specify 3 for <code>lport</code> and 4 for <code>count</code>, the output shows entries for logical ports 3, 4, 5, and 6. If you specify 14 for <code>lport</code> and 5 for <code>count</code>, the output is truncated to show ports 14, 15, and 16. If no value is specified, the output displays information only for the logical port specified. <code>rspslot</code> is the RSP slot number—1 or 2. When you specify an RSP slot number, you must also set a nonzero value for <code>count</code>. If you do not specify a value for <code>rspslot</code>, the system uses the default RSP slot number.

Command element	Description
	■ <code>rspglobal [rspslot]</code>—Route Switch processor's global statistics. ■ <code>sch sid[count count rspslot]</code>—Scheduler statistics. <i>sid</i> is the scheduler ID. <i>count</i> specifies the number of entries to display. Valid values are from 1 through 16. If you specify 3 for <i>lport</i> and 4 for <i>count</i>, the output shows entries for logical ports 3, 4, 5, and 6. If you specify 14 for <i>lport</i> and 5 for <i>count</i>, the output is truncated to show information for logical ports 14, 15, and 16. If no value is specified, the output displays information only for the logical port specified. <i>rspslot</i> is the RSP slot number—1 or 2. When you specify an RSP slot number, you must also set a nonzero value for <i>count</i>. ■ If you do not specify a value for <i>rspslot</i>, the system uses the default RSP slot number.

Example The following command enables statistics collection on all the Ethernet ports:

```
admin> stats enable ether all
Statistics collection enabled for ether port 1
Statistics collection enabled for ether port 2
```

Example The following sample command enables statistics collection on a specific Ethernet port, in this example, Ethernet port 1:

```
admin> stats enable ether 1
Statistics collection enabled for ether port 1
```

Example The following command disables statistics collection from all Ethernet ports:

```
admin> stats disable ether all
Statistics collection disabled for ether port 1
Statistics collection disabled for ether port 2
```

Example The following command clears statistics for all Ethernet ports:

```
admin> stats clear ether all
Port 1 Cleared
Port 2 Cleared
```

Example To display traffic statistics on a specific Ethernet port, append the port number to the `stats traffic ether` command. For example:

```
admin> stats traffic ether 1
Rx frames      : 21647      Tx frames      : 21222
Rx bytes       :1385748    Tx bytes      : 1443416
Rx multicast   :2          Tx multicast   : 2
Rx broadcast   : 21642     Tx broadcast  : 21217
Rx MAC pause   : 0         Tx MAC pause   : 0
Rx IW frames   : 30271     Tx control    : 0
Rx Host frames : 5         Tx Host frames : 5
```

Example To show the error statistics on all ethernet ports, enter the `stats error ether` command. For example:

```
admin> stats error ether
PORT Rx FCS    Tx FCS    Rx Drop    Tx Drop    Rx Mac    Tx SColl
1    0          0          0          0          0          0
2    0          0          0          0          0          0
```

status

Description Displays the status windows. You can configure the content of the windows to show connection, line, or log-message information.

Permission level system

Usage status [on | off]

Command element	Description
on	Display the status windows.
off	Hide the status windows.

Example To display status windows:

```
admin> status

or

admin> status on
```

```

2 Connections
001 tomw TCP 1/7/14 19200
002 timl TCP 1/7/3 56000

Status
Serial number: 6201732   Version: 9.0F
Rx Pkt:    11185897
Col:       129
12/26/2002 12:20:15 Up:    3 days, 21:47:32
M: 29 L: info Src: shelf-1/controller

Issued: 16:48:02, 09/27/2002

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

```

To hide the windows:

```
admin> status
```

or

```
admin> status off
```

See Also connection, log, view

T

telnet

Description Opens a telnet session across the network to the specified host.

Permission level diagnostic

Usage telnet [-a | -b | -t] [-l [e] | -r [e]] hostname [portnumber]

Command element	Description
-a	ASCII mode, or standard 7-bit mode. In 7-bit mode, bit eight is set to 0 (zero). This value is the default if no other mode is specified.
-b	Binary mode. The Stinger unit attempts to negotiate the telnet 8-bit binary option with the server at the remote end. You can run X-Modem and other 8-bit file transfer protocols in this mode.
-t	Transparent mode. You can send and receive binary files, and run the same file-transfer protocols, without having to be in binary mode.
-l [e]	Local echo. As you type a line, it echoes on your terminal screen, but is not actually transmitted until you enter a carriage return.
-r [e]	Remote echo. Turn local echo off.

Command element	Description
hostname	IP address or Domain Name System (DNS) name of a networked host.
portnumber	Port number for telnet sessions. The default port is 23.

Example To open a telnet session to host-231:

```
admin> telnet host-231
Connecting to host-231 (10.65.12.231) ...
Escape character is '^]'
Connected
```

You can also open a session after starting the telnet program. To display the available commands:

```
admin> telnet
telnet> ?
?                Displays this information.
help             "      "      "
open             Connect to a site.
quit             Quit Telnet.
close            Close current Telnet connection.
send             Send Telnet command. Type 'send ?' for help.
set              Set special char. Type 'set ?' for help.
```



Note During an open telnet connection, type the Ctrl key plus a right square bracket (Ctrl+]) to display the telnet> prompt and the telnet command-line interface. Any valid telnet command returns you to the open session. Note that Ctrl+] does not function in binary mode telnet. If you log into the Stinger unit by telnet, you might want to change its escape sequence from Ctrl+] to a different setting.

See Also ping

terminal-server

Description Starts terminal-server mode, which has its own command interface.

Permission level termserv

Usage terminal-server

Example To enter terminal-server mode and display the list of available commands:

```
admin> terminal-server
admin% ?
?                Display help information
help             "      "      "
quit             Closes terminal server session
hangup           "      "      "      "
local            Go to local mode
remote           remote <station>
```

set	Set various items. Type 'set ?' for help
show	Show various tables. Type 'show ?' for help
iproute	Manage IP routes. Type 'iproute ?' for help
telnet	telnet [-a -b -t] <host-name> [<port-number>]
tcp	tcp <host-name> <port-number>
ping	ping <host-name>
traceroute	Trace route to host. Type 'traceroute -?' for help
rlogin	rlogin [-l user -ec] <host-name>

To exit terminal server mode:

```
admin% quit
```

```
admin>
```

See Also ping, telnet

thermalstatus

Description Displays a number of temperature-related values to show the overall thermal status of the unit. The values include:

- Ambient temperature at fan tray intake.
- Shelf-controller temperature.
- High, low, and alarm temperature thresholds.
- Slot-card temperature for slot cards that support temperature reporting. Currently, no slot cards support thermal information reporting.
- Power supply thermal status, and whether the power supplies are in an overheated state.
- Fan tray status, including the fan tray operational mode, low-noise speed in revolutions per minute (RPM), current fan mode, and current speed of each fan in RPMs.

Permission level system

Usage thermalstatus

Example To display the overall thermal status of the unit:

```
admin> thermalstatus
System Thermal status
Ambient temperature at intake : 27 C (80 F)
Shelf controller temperature  : 35 C (95 F)
High temperature threshold   : 36 C (96 F)
Low temperature threshold    : 32 C (89 F)
Alarm temperature threshold  : 38 C (100 F)
Slot cards:
(no slot cards contain thermal information)
```



```
Power supply thermal status
Power Supply #      Temp
=====
A                   OK
B                   OK
C                   n/a
D                   OK
```

```
Fantray status
Fan operational mode: auto-regulation
Low-noise RPM:      2000
Current fan mode:   Full-speed
Fan #              RPM              Status
=====
1                  3289              GOOD
2                  3214              GOOD
3                  3075              GOOD
4                  3143              GOOD
5                  3214              GOOD
6                  3289              GOOD
```

topology

Description Displays the topology of a hosted Stinger MRT system.

Permission level diagnostic

Usage topology [-p | -d | -s | -r] Shelf_ID

Command element	Description
With no options	Display the entire topology.
-p	Display a pictorial view of the topology.
-d shelf	Display the topology details of a shelf.
-s shelf	Display the statistics of a shelf.
-r shelf	Send an init packet from the host to a remote shelf without resetting the shelf.

Example In the following example, remote shelf 3 is connected to EXP1, and no remote shelves are connected after it. On EXP2 remote shelf 2 is connected, followed by remote shelf 5.

```
admin> topology
Slaves connected to EXP1 of Master
=====
ShelfId              : 3
Operational State    : UP
Admin State          : UP
Position             : 1
MrtType              : STINGER_MRT_23INCH_PLATFORM
MRT Connected to Exp1 : 1
```

```
MRT Connected to Exp2      : 16
Port connected to - On Master : 0
Port connected to - On Slave  : 0
```

Slaves connected to EXP2 of Master

```
=====
ShelfId                      : 2
Operational State           : UP
Admin State                  : UP
Position                     : 1
MrtType                      : STINGER_MRT_23INCH_PLATFORM
MRT Connected to Exp1       : 1
MRT Connected to Exp2       : 5
Port connected to - On Master : 1
Port connected to - On Slave  : 0
```

```
ShelfId                      : 5
Operational State           : UP
Admin State                  : UP
Position                     : 2
MrtType                      : STINGER_MRT_23INCH_PLATFORM
MRT Connected to Exp1       : 2
MRT Connected to Exp2       : 16
Port connected to - On Master : 1
Port connected to - On Slave  : 0
```

Field	Description
ShelfId	ID of the remote shelf.
Operational State	Operational state of the remote shelf.
Admin State	State set by the administrator, either in a profile or by using a command.
Position	Position of the remote shelf relative to the host.
MrtType	Description of the Stinger MRT platform.
MRT Connected to Exp1	ID of shelf connected to that EXP1 port. The string ANY-SHELF indicates an invalid shelf ID. The number 16 indicates that no remote shelf is connected to the port.
MRT Connected to Exp2	ID of shelf connected to that EXP2 port. The string ANY-SHELF indicates an invalid shelf ID. The number 16 indicates that no remote shelf is connected to the port.
Port connected to - On Master	The cascade port used by the host to connect to the remote shelf. The string ANY-PORT indicates an invalid port number.
Port connected to - On Slave	The cascade port used by the remote shelf to connect to host. The string ANY-PORT indicates an invalid port number.

Example For a picture of the topology, use the `topology -p` command. For example:

```
admin> topology -p
```



Example You can also display the details about a particular shelf by using the `topology -d` command and specifying the remote shelf ID. For example:

```
admin> topology -d 5
ShelfId           : 5
Operational State  : UP
Admin State       : UP
Position          : 2
MrtType           : STINGER_MRT_23INCH_PLATFORM
MRT Connected to Exp1 : 2
MRT Connected to Exp2 : 16
Port connected to - On Master : 1
Port connected to - On Slave  : 0
```

Example To display statistics about the types of packets received and sent to a particular shelf, use the `topology -s` command with the remote shelf ID. For example:

```
admin> topology -s 3
Statistics of Shelf: 3
discovery restart          : 0
Number of requests received
Valid                      : 1
Duplicate ShelfId         : 0
Admin State not UP: 0
Invalid                   : 0
Discarded                 : 0
Number of Ack Sent        : 1
Number of Nack Sent       : 0
Number of Reset Sent      : 0
Number of Init Sent       : 0
```

Field	Description
discovery restart	Number of times autodiscovery has been restarted.
Number of requests received	

Field	Description
Valid	Count of valid requests received.
Duplicate ShelfId	Another MRT sent requests with this shelf ID.
Admin State not UP	Request was received when administrative state for this shelf was down or unknown.
Invalid	An invalid request was received. A request is invalid if it contains a protocol ID or version mismatch, or is sent from invalid intermediate shelf.
Discarded	Request discarded, which might indicate that the intermediate shelf is down.
Number of Ack Sent	Number of Acks sent to the shelf.
Number of Nack Sent	Number of Nacks sent to the shelf.
Number of Reset Sent	Number of Resets sent to the shelf.
Number of Init Sent	Number of Inits sent to the shelf.

Example When you specify shelf ID 1, indicating the host, the `topology -s` command displays the number of erroneous packets received. For example:

```
admin> topology -s 1
Discarded packets      : 0
Request Rcvd with Invalid ShelfID    : 0
```

Field	Description
Discarded packets	Packets discarded due to header errors, intermediate shelves being down. No action had been taken on these packets, they were silently discarded.
Request Rcvd with Invalid ShelfID	Autodiscovery received from with invalid shelf ID (a shelf ID outside the range from 2 to 7).

Example If you execute the `topology -s` command on the remote shelf, statistics are displayed for that shelf only. For example:

```
admin> open 3 8
SLAVE3/8>> topology -s
Statistics of Shelf: 3
Discarded packets      : 0
Discovery restart      : 0
Number of Req Sent     : 126
Number of Ack Rcvd     : 0
Number of Nack Rcvd    : 0
Number of PassThruReq  : 0
Number of PassThruRep  : 0
Number of Init Rcvd    : 0
Number of Reset Rcvd   : 0
```

Field	Description
Discarded packets	Packet discarded due to header errors.
Discovery restart	Number of times Auto Discovery has been restarted.
Number of Req Sent	Number of Auto Discovery Request sent.
Number of Ack Rcvd	Number of Acks received from the host.
Number of Nack Rcvd	Number of Nacks received from the host.
Number of PassThruReq	Number of pass through request forwarded.
Number of PassThruRep	Number of pass through replies forwarded.
Number of Init Rcvd	Number of Inits received from the host.
Number of Reset Rcvd	Number of Resets received from the host.

Example Usually, the host sends an init packet to a remote shelf only if its administrative state is UP and its operational state is DOWN. To restart autodiscovery between the host and a remote shelf without resetting the shelf, use the `topology -r` command and specify the shelf's ID. For example:

```
admin> topol -r 2
```

traceroute

Description Traces the route an IP packet follows by launching User Datagram Protocol (UDP) probe packets with a low time-to-live (TTL) value and then listening for an Internet Control Message Protocol (ICMP) time exceeded reply message from a router. Probes start with a TTL of 1 (one) and increase by 1 until either a probe packet reaches the destination host or the TTL reaches the maximum.

Three probes are sent at each TTL setting. The second line of command output shows the address of the router and round-trip time of each probe. If the probe answers come from different gateways, the address of each responding system is printed. If the Stinger unit receives no response within a 3-second timeout interval, the command output is an asterisk (*).

The destination host is not supposed to process the UDP probe packets, so the destination port is set to an unlikely value, such as 33434. When the packets reach the destination host, it sends back an ICMP port unreachable message.

Permission level diagnostic

Usage `traceroute [-n] [-v] [-m max_ttl] [-p port] [-q nqueries] [-w waittime] [-s src_IPaddr] hostname [datasize]`

Command element	Description
-n	Print hop addresses numerically rather than symbolically and numerically. (This option eliminates a name server address-to-name lookup for each gateway found on the path.)

Command element	Description
-v	Verbose output. Include received ICMP packets other than time exceeded and ICMP port unreachable.
-m max_ttl	Maximum TTL (maximum number of hops) used in outgoing probe packets. The default is 30 hops.
-p port	Base UDP port number used in probes. If a device is listening on a port in the default range, this option can be used to pick an unused port range. The default is 33434.
-q nqueries	Maximum number of queries for each hop. The default is 3.
-w waittime	Time to wait for a response to a query. The default is 3 seconds.
-s src_IPaddr	IP address of the source host.
hostname	IP address or Domain Name System (DNS) name of a networked host.
datasize	Size of the data field of the UDP probe datagram sent by traceroute. The default is 0 (zero), which results in a datagram size of 38 bytes (a UDP packet carrying no data).

Example To trace the route to host-231:

```
admin> traceroute host-231
traceroute to host-231 (10.65.12.231), 30 hops max, 0 byte packets
 1 host-231.abc.com (10.65.12.231) 0 ms 0 ms 0 ms
```

To perform the same trace, but with a maximum TTL of 60 hops:

```
admin> traceroute -m 60 host-231
traceroute to host-231 (10.65.12.231), 60 hops max, 0 byte packets
 1 host-231.abc.com (10.65.12.231) 0 ms 0 ms 0 ms
```

The following annotations can appear in the command output after the time field:

Output annotation	Description
!H	Host reached.
!N	Network unreachable.
!P	Protocol unreachable.
!S	Source route failed. Occurrence of this event might indicate a problem with the associated device.
!F	Fragmentation needed. Occurrence of this event might indicate a problem with the associated device.
!?	ICMP subcode. The event indicates an error.

Output annotation

!??

Description

Reply received with inappropriate type. The event indicates an error.

See Also ping, netstat

U

uptime

Description Reports the number of days, hours, minutes, and seconds the system and individual modules have been active (in the Up state).

Permission level system

Usage uptime [[-a] | [[shelf] slot]]

Command element**Description**

No options

Display the system uptime.

-a

Display the time all modules in the Up state have been active.

slot

Display the amount of time for the specified module on the master shelf has been active.

shelf slot

Display the amount of time for the module specified by shelf and slot has been active (Up).

Example The following example shows the amount of time that all modules in the Up state have been active. (Modules that are not in the Up state are not reported.)

```
admin> uptime -a
17:50:44
{ shelf-1 slot-4 } al-dmtadsl-atm-card      0 days 02:45:42    8.0a0e0
{ shelf-1 slot-6 } sdsl-atm-card           0 days 02:45:48    8.0a0e0
{ shelf-1 control-module } shelf-controller 0 days 02:47:05    8.0a0e0
```



Note To enable network management stations to obtain uptime information, the following SNMP variable has been added to the Ascend Enterprise Management Information Base (MIB):

```
slotLastChange  OBJECT-TYPE
    SYNTAX      TimeTicks
    ACCESS      read-only
    STATUS      mandatory
    DESCRIPTION  "The value of sysUpTime at the time the slot card
                  entered its current state."
    ::= { slotEntry 9 }
```

The slotLastChange variable reports the value of sysUpTime at the time the module entered its current state.

usergroupcheck

Description Enables validation of user and group specifications.

Permission level system

Usage usergroupcheck [-u user | -g group] [-a]

Command element	Description
-u user	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.
-g group	Verify that the user-group profile specified by group specifies a valid list of commands. If the command user group contains commands that are valid on a module, this option displays the commands.
-a	Verify that all user-group profiles specify valid lists of commands, and that all user-group profiles specified by user profiles are valid.

Example For example, to verify the user-group profile specified in the user profile called bill:

```
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 )
```


Example To verify that the `newyork` command user group contains a valid list of commands:

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

Example To verify that all user-group profiles specify valid lists of commands, and that all user-group profiles specified by user profiles are valid:

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

userstat

Description Displays user session status.

Permission level system

Usage `userstat` `[[ -s | -t | -k sessionID | -a ipAddress | -u username | -l | -d ]`
`[-o format]] .`

Command element	Description
No options	Display user session status.
-s	Show users (default).
-t	Show the total number of active users.
-k sessionID	Terminate a user session.
-a ipAddress	Show the session with a matching IP address.
-u username	Show the session with a matching username.
-l	Display the output in wide format (more than 80 characters).
-d	Dump the session. Do not pass session output through more format values.
-o format	Show only the details specified. By default, all information is displayed. Replace format with one or more of the following to focus the display: ■ %i—Session ID ■ %l—Physical address (Line/chan) ■ %s—Location (Slot:Item) ■ %r—Transmit and receive rates (Tx/Rx rate) ■ %d—Type of service (Svc) ■ %a—Address ■ %u—Username ■ %c—Connection time ■ %t—Idle time ■ %n—Dialed number

Example To display user session status:

```
admin> userstat
SessionID Line/Chan Slot:Item Tx/Rx Rate Svc Address Username
228687860 1.01.02/01 1:03:01/01 56K/56K TCP 10.100.0.1 barney
228687861 1.02.03/02 1:04:02/00 28800/33600 TCP 10.168.6.24 jake
<end user list> 2 active user(s)
```

The display output contains the following fields:

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	Location (Shelf:slot:item/logical-item) of the host port to which the call was routed.
Tx/Rx Rate	Transmit and receive rates.
Svc	Type of service in use for the session. Following are the possible values: ■ ----(The service is being negotiated.) ■ SLP—Serial line IP ■ TLN—telnet ■ BTN—Binary telnet ■ TCP—Raw Transmission Control Protocol (TCP) ■ TRM—Terminal server ■ VCN—Virtual connect ■ DTP—DTPT
Dialed#	The number dialed to initiate this session. (This information appears only when you use the -l option.)
ConnTime	The amount of time (in hours:minutes:seconds format) since the session was established. (This information appears only when you use the -l option.)
IdleTime	The amount of time (in hours:minutes:seconds format) since data was last transmitted across the connection. (This information appears only when you use the -l option.)

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
228687860 1.01.02/01
228687861 1.02.03/02
<end user list> 1 active user(s)
```

Example To terminate a user session, include the `-k` option and session ID with the `userstat` command:

```
admin> userstat
SessionID Line/Chan Slot:Item Rate Svc Address Username
246986325 1.01.02/01 1:13:01/000 33600 TCP 100.100.8.2
100.100.8.2
<end user list> 1 active user(s)

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

Example To display the total number of active users enter the `userstat` command with the `-t` option. For example:

```
admin> userstat -t
2 active user(s)
```

V

vdslines

Description Displays the status of all very-high-bit-rate digital subscriber lines (VDSL).

Permission level system

Usage `vdslines [ -a | -d | -f | -sh shelf | -sl shelf slot | -u ]`

Command element	Description
<code>-a</code>	Show all VDSL lines.
<code>-d</code>	Show disabled lines.
<code>-f</code>	Show all free lines.
<code>-sh shelf</code>	Limit the output to lines on the specified shelf.
<code>-sl shelf slot</code>	Limit the output to lines on the specified slot.
<code>-u</code>	Show in-use lines.

Example To show all free lines:

```
admin> vdslines -f
Free VDSL lines:
Line      { 1 4 3 } (dvOp dvUpSt dvRq sAdm nailg)
Line      { 1 4 4 } (Down Idle UP UP 00153)
Line      { 1 4 4 } (Up Idle UP UP 00154)
```

The data displayed includes the physical address of each line and the following status information:

Field	Description
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 operations mode.
sAdm	Desired administrative state of the line: ■ Down specifies that the line should terminate all operations and enter the deactivated state. ■ Up specifies that the line should be activated in normal operations mode. The 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 (for example, someone has dialed in) that should change the Stinger unit to the desired state.
na1lg	Dedicated (nailed) group to which the line is assigned.

version

Description Displays the current system software version, control module revision number, and control module model number.

Permission level system

Usage version

Example To display version information:

```
admin> version

Software version 9.2-167
* * * 9_2-167/stngrcm2 <satishb> Jun 01 2002 04:09 * * *
Hardware revision: 2.0 Model A
```

Dependencies If no hardware revision is displayed, a revision 1 control module is present and is running a software version earlier than TAOS 9.1-142. The system displays the control module model number only if a revision 2 control module is present.

view

Description Changes the information displayed in the top or bottom status window.

Permission level system

Usage view position status-type

Command element	Description
position	Area of the status window to be affected by the command: ■ top ■ bottom ■ left
status-type	Type of status information to display. ■ If the specified window position is top or bottom, the window can display one of the following types of status information: – general—General status information – log—32-message log buffer – line—Line and channel status ■ If the specified window position is left, the window can display one of the following types of status information: – connection—WAN connection status – session—Management status

Example To display session information:

admin> view left session

3 Sessions	1/13/8	RA
console		
admin 135.254.196.37		
pratul 135.254.196.37		
M: 48 L: info Src: shelf-1/controller		
Issued: 16:48:02, 09/27/2002		
[Next/Last Conn:<dn/up arw>, Next?Last Page: <pg dn/up>, Exit: <esc>]		

See Also connection, ledoff, log

vrouter

Description Displays entries in the virtual router (VRouter) table.

Permission level system

Usage vrouter [dump [full]]

Command element	Description
dump	Display the entries in the VRouter table.
full	Display extended information about the entries in the VRouter table.

Example To display VRouter table entries:

```
admin> vrouter dump
Total number of VRouters = 1
Index = 1, Name = cli, ID = 1
```

W

wandisplay

Description Specifies the number of bytes of a WAN message display.

Permission level diagnostic

Usage wandisplay n

Command element	Description
n	Number of bytes to display. A 0 (zero) turns off the display.

Example To display the first 25 bytes of each WAN message:

```
admin> wandisplay 25
Display the first 25 bytes of WAN messages
```

See Also wanopening, wandsess

wandsess

Description Enables you to specify the number of bytes to display for a single WAN session.

Permission level diagnostic

Usage wandsess sess n

Command element	Description
sess	Local or RADIUS profile name used to specify the session.
n	Number of bytes to display.

Example admin> wandsess tim 120

admin> wandsess bob 160

```
admin> wandsess
      120    tim
      160    bob
```

See Also wandisplay, wannext, wanopening

wannext

Description Specifies the number of bytes of a WAN message to display for the next call only.

Permission level diagnostic

Usage wannext n

Command element	Description
n	Number of bytes to display. A 0 (zero) turns off the display.

Example To display 25-byte WAN messages for the next call:

admin> wannext 25

Display the first 25 bytes of WAN messages for the NEXT call

See Also Wandisplay, wandsess, wanOpening

wanopening

Description Specifies the number of bytes of a WAN opening message to display.

Permission level diagnostic

Usage wanopening n

Command element	Description
n	Number of bytes to display. A 0 (zero) turns off the display.

Example To display 50 bytes of each WAN opening message:
admin> wanopening 50
Display the first 50 bytes of WAN messages during OPENING only

See Also wandisplay, wandsess

which

Description Enables you to look up the dedicated (nailed) group associated with the port used for an Asynchronous Transfer Mode (ATM) connection.

Permission level system

Usage which [-p | -n] [-c] port | group [ifType]

Command element	Description
-p	Show the port—and channel, for the IDSL line interface module (LIM)—associated with the dedicated (nailed) group indicated by group.
-n	Show the dedicated (nailed) group or groups associated with the port indicated by port, in {shelf slot item} format.
-c	List the connections associated with the nailed group or port.
port	Physical address of the port.
group	Dedicated group number.
ifType	IANA interface type.

Example To display the port associated with dedicated (nailed) group 21:

```
admin> which -p 21
The port corresponding to nailed group 21 is:
{ shelf-1 slot-1 21 }
```

Add the -c option to include a display of the connections associated with this dedicated (nailed) group:

```
admin> which -p -c 21
The port corresponding to nailed group 21 is:
{ shelf-1 slot-1 21 }
The connection(s) associated with this nailed group are:
lim-1-21-ckt-1
lim-1-21-ckt-8
lim-1-21-ckt-7
lim-1-21-ckt-6
lim-1-21-ckt-5
lim-1-21-ckt-4
lim-1-21-ckt-3
lim-1-21-ckt-2
```

Example To display the dedicated (nailed) group corresponding to port 1 of an IDSL module in slot 13:

```
admin> which -n {1 13 1}
Nailed group corresponding to port { shelf-1 slot-13 idsl-1 channel 1 } is
601
Nailed group corresponding to port { shelf-1 slot-13 idsl-1 channel 2 } is
601
Nailed group corresponding to port { shelf-1 slot-13 atm-internal-1 } is 633
```



Note For the IDSL line interface module (LIM), the dedicated (nailed) groups assigned to both BRI channels and the dedicated (nailed) group assigned to the ATM interface are displayed. The ATM Internal interface has the same physical address as the first BRI channel. The IDSL line is identified by `idsl-` before the line number. The ATM Internal interface is identified by `atm-internal-` before the line number.

Example You can use the `which` command to determine which port is in use when you have the dedicated (nailed) group assignment of a connection profile. For example, if the circuit uses nailed-group 296:

```
admin> which -p 296
The port corresponding to nailed group 296 is: { shelf-1 slot-6 46 }
```

In the case of the port on an IDSL card, if the circuit uses nailed-group 601, and nailed-group 633 as its ATM internal interface:

```
admin> which -p 601
The port corresponding to nailed group 601 is:
{ shelf-1 slot-13 idsl-1 chan-1 }
{ shelf-1 slot-13 idsl-1 chan-22 }

admin> which -p 633
The port corresponding to nailed group 633 is: { shelf-1 slot-13
atm-internal-1 }
```

Example If the argument specifies a slot that is not populated, or a dedicated (nailed) group that is not assigned, the command returns a message that the number was not found. For example:

```
admin> which -p 43
The port corresponding to nailed group 43 is:
NONE!
```

Example If more than one port has the same dedicated (nailed) group associated with it (which is illegal), the which command returns all the ports that have this dedicated (nailed) group. Using the which command can be a convenient way to find duplicate dedicated (nailed) groups. For example:

```
admin> read sdsl {1 6 46}
SDSL/{ shelf-1 slot-6 46 } read
admin> set line-config nailed-group=801
admin> write
SDSL/{ shelf-1 slot-6 46 } written
admin> which -p 801
The port corresponding to nailed group 801 is:
{ shelf-1 slot-6 46 }
{ shelf-1 trunk-module-1 1 }
```

Duplicate dedicated (nailed) group assignments can occur only when you change default nailed-group numbers. To fix the problem, change the dedicated (nailed) group assignments in one or more profiles, and then verify by using the which command again.

Dependencies The following rules apply when using the which command:

- If you enter a physical address, the system assumes the logical item to be zero.
- If you do not enter an IANA interface type, the system attempts to guess the IANA type of the given address.
- For an IDSL port, the format {{ shelf slot item}0} represents an entire line.

who

Description Enables you to display information about or disconnect administrative users.

Permission level system

Usage who [am i] | [-k username IPaddress]

Command element	Description
No options	Display the names of administrative users, user profiles, and IP addresses of administrative users from telnet sessions.
am i	Display the current user and user profile for an administrative session.
-k username IPaddress	Disconnect an administrative session for a specified user at a specified IP address.

Example Without any arguments, the output of the 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
```

To display the current user and user profile for an administrative session, use the `who am i` command. The output of this command is similar to the existing `whoami` command. For example:

```
admin> who am i
User Name : admin      User Profile : admin
```

To disconnect an administrative session, use the `-k` option with the `who` command. For example, the following command disconnects the user `pratul` logged in from IP address `200.254.96.37`:

```
admin> who -k pratul 200.254.196.37
LOG critical, Shelf 1, Controller-1, Time: 05:24:17--
user admin from 200.254.196.37 disconnected user pratul from 135.254.196.37
1 administrative user killed.
```

The preceding command disconnects all sessions with the user name `pratul` logged in from IP address `200.254.96.7`.

Dependencies 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`.

whoami

Description Displays the name of the user profile associated with the current session.

Permission level `user`

Usage `whoami`

Example To display the name of your user profile:

```
admin> whoami
tommy
```

See Also `auth`

write

Description Validates the settings of the working profile and then writes it from the edit buffer to nonvolatile RAM (NVRAM).

If you modify a profile and do not use the write command before reading another profile, the changes are lost.

Permission level update

Usage write [-f]

Command element	Description
-f	Force the write operation without prompting for confirmation, overwriting an existing profile if one exists with the same index.

Example To create a new connection profile, modify it, and write it to NVRAM:

```
admin> new conn newyork
CONNECTION/newyork read

admin> list
[in CONNECTION/newyork (new)]
station*=newyork
active=no
encapsulation-protocol=atm
called-number-type=national
dial-number=""
clid=""
ip-options={ yes yes 0.0.0.0/0 0.0.0.0/0 7 100 255 no no 0 +
session-options={ "" "" no 120 no-idle 120 "" }
telco-options={ ans-and-orig no off 1 no no 56k-restricted 0 +
usrRad-options={ global 0.0.0.0 1646 "" 1 acct-base-10 }
calledNumber=""

admin> write
CONNECTION/newyork written
```

Dependencies Consider the following:

- If the working profile has an index field—a parameter followed by an asterisk(*)—that parameter must have a value or the write operation is not allowed.
- If you issue a write command when the current profile has not been modified from the saved version, the write does not occur and the following message is displayed:

```
admin> write
Nothing new to write; nothing written.
```

You can force the write to occur by using the -f option on the write command line.



Note The write always occurs if the profile has not been written previously.

See Also list, new, read, set

Stinger Profile Reference



2

A..... 2-2

B..... 2-18

C..... 2-22

D..... 2-31

E..... 2-37

F..... 2-40

G..... 2-45

H..... 2-46

I..... 2-48

L..... 2-62

M..... 2-72

N..... 2-76

O..... 2-78

P..... 2-84

Q..... 2-98

R..... 2-100

S..... 2-106

T..... 2-117

U..... 2-129

V..... 2-131

W..... 2-134

X..... 2-135

access-properties

Usage Following is a listing of the `access-properties` subprofile with its default settings:

action

Usage Following is a listing of the `action` subprofile with its default settings:

addr-index

Usage Following is a listing of the `addr-index` subprofile with its default settings:

```
[in PNNI-SUMMARY-ADDR/"":addr-index (new)]
node-index = 0
type = internal-summary
address = 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
prefix-len = 0
```

ADMIN-STATE-PERM-IF

Description A read-only profile that holds information about the Stinger dedicated (nailed) interfaces. The system creates a profile for an active dedicated interface and assigns it an interface index.

Usage Read-only. Following is a sample listing of the admin-state-perm profile:

```
[in ADMIN-STATE-PERM-IF/frdevice1]
station*=frdevice1
snmp-interface=19
desired-state=admin-state-up
desired-trap-state=trap-state-enabled
inet-profile-type=1
```

ADMIN-STATE-PHYS-IF

Description A read-only profile that indicates information about the system's physical interfaces. The system creates a profile for each of its physical interfaces.

Usage Read-only. Following is a sample listing of the admin-state-phys-if profile:

```
[in ADMIN-STATE-PHYS-IF/{ shelf-1 slot-1 1 }]
device-address* = { shelf-1 slot-1 1 }
slot-type = dadsl-atm-24-card
snmp-interface = 13
modem-table-index = 0
desired-state = admin-state-down
desired-trap-state = trap-state-enabled
```

ADSL-BIN-LOADING

Description A profile that enables you to configure frequency bin-loading settings for ADSL lines. You mask or disable an unwanted frequency using the bin-loading parameter. The AL-DMT:bin-loading subprofile displays the adsl-bin-loading profile configured for a specific ADSL line.

Usage Following is a listing of the adsl-bin-loading profile with its default settings:

```
[in ADSL-BIN-LOADING/default (new)]
name* = default
bits-per-bin = 14
bin-loading = [ yes yes yes yes yes yes yes yes yes yes yes yes+]
```

ALARM

Description A profile that enables you to configure the unit's status lights (LEDs) and alarm relays to respond to specific conditions.

Usage Following is a listing of the alarm profile with its default settings:

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



Note You can configure default ALARM profiles that apply to the entire Stinger unit by setting the physical-address parameter to { 0 0 0 } (any shelf, any slot, any item).

See Also action

alarm-id

Description A subprofile that identifies an alarm by shelf and module.

Usage Following is a listing of the alarm-id subprofile with its default settings:

```
[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
```

See Also alarm (command), ALARM-STAT

ALARM-STAT

Description A read-only profile that indicates the status of alarms. When there are alarms, alarm-stat parameters are created. The profile lists an alarm-id subprofile for each of the alarms that have occurred. The alarm-id subprofile consists of the physical address of the device that has the alarm condition and an indication of the alarm event.

Usage Read-only. Following is a sample listing of the alarm-stat profile:

```
[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
```

See Also alarm-id

AL-DMT

Description A profile that enables you to configure each of the 12 asymmetric digital subscriber line (ADSL) ports on each installed Asynchronous Transfer Mode (ATM) ADSL line interface module (LIM).

Usage Following is a listing of an al-dmt profile for the device on shelf 1, slot 4 with its default settings:

```
[in AL-DMT/{ shelf-1 slot-4 1 }]
name=1:4:1
physical-address*={ shelf-1 slot-4 1 }
enabled=yes
sparing-mode = inactive
ignore-lineup = system-defined
line-config={ 0 301 static { any-shelf any-slot 0 } +
fast-path-config={ 10 50 1000 8000 200 1000 }
interleave-path-config={ 0 0 0 0 0 0 16 16 }
margin-config={ 6 6 0 0 31 31 0 0 0 0 0 0 0 }
thresh-profile = default
bin-loading-profile = default
```

AL-DMT-STAT

Description A read-only profile that provides statistics and connection status for each rate adaptive digital subscriber line (RADSL) interface.

Usage Read-only. Following is a sample listing of the al-dmt-stat profile:

```
[in AL-DMT-STAT/{ shelf-1 slot-4 1 }]
physical-address* = { shelf-1 slot-4 1 }
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-0-7-vci-32-255
vp-switching-vpi = 7
physical-status = { 155 coe port-up 0 0 512000 2336000 interleave +
physical-statistic = { { 4 1 43 } yes 2 passed 4 7 3 6 0 11 40142 231 65 +
```

ANSWER-DEFAULTS

Description A profile that enables you to configure system defaults for incoming session requests. The system uses the values in this profile before it answers an incoming call. The values you set override factory defaults.

Usage Following is a listing of the answer-defaults profile with its default settings:

```
[in ANSWER-DEFAULTS]
use-answer-for-all-defaults = yes
force-56kbps = no
profiles-required = yes
clid-auth-mode = ignore
clid-selection = first
ppp-answer = { yes no-ppp-auth none "" yes 0 none 1524 no 600 600 1524+
mp-answer = { yes 1 2 }
mpp-answer = { yes quadratic transmit 1 1 15 5 10 70 }
fr-answer = { yes }
tcp-clear-answer = { yes }
ip-answer = { yes yes no 1 no }
session-info = { "" "" no 120 no-idle 120 0 }
atm-answer = { }
```

Dependencies Consider the following:

- Similar settings in a client's profile, which are applied after a call has been authenticated, always override the default settings in this profile.
- The following answer-defaults entries do not apply to Stinger units:

```
force-56kbps = no
clid-auth-mode = ignore
clid-selection = first
mp-answer = { yes 1 2 }
mpp-answer = { yes quadratic transmit 1 1 15 5 10 70 }
tcp-clear-answer = { yes }
```

answer-options

Description A subprofile that enables you to configure answering procedures within a connection profile.

Usage Following is a listing of the answer-options subprofile with its default settings:

```
[in CONNECTION/":answer-options (new)]
profile-required = no
ans-default = no
profile-flags = no
clid-auth-mode = ignore
clid-selection = first
```

APS-CONFIG

Description A profile that enables you to configure the protection group in a channel that uses automatic protection switching (APS). The protection group is created for each OC3-ATM trunk port on the trunk aggregation module when the `aps-config` profile is configured and activated, and is referred to from an `oc3-atm` profile by its `aps-config-name` parameter.

Usage Following is a listing of an `aps-config` profile named `pg1` with its default settings:

```
[in APS-CONFIG/pg1 (new)]
name = pg1
active = no
linear-protection-channel = { 1 trunk-module-1 2 }
protection-mode = 1+1
direction-mode = bidirectional
revertive-mode = revertive
wtr-timer-duration = 30000
psbf-failure-timer-duration = 250
psbf-clear-timer-duration = 1000
mode-mismatch-failure-timer-duration = 250
mode-mismatch-clear-timer-duration = 1000
channel-mismatch-failure-timer-duration = 250
channel-mismatch-clear-timer-duration = 1000
fepl-mismatch-failure-timer-duration = 250
fepl-mismatch-clear-timer-duration = 1000
protection-channel-signal-degrade-exponent = 6
protection-channel-signal-failure-exponent = 3
working-channel-signal-degrade-exponent = 6
working-channel-signal-failure-exponent = 3
```

APS-STAT

Description A read-only profile that is created whenever a protection group is activated. The profile is indexed by the protection group's name.

Usage Read-only. Following is a sample listing of an `aps-stat` profile called `pg1`:

```
[in APS-STAT/pg1]
name = pg1
protection-channel = { shelf-1 trunk-module-1 2 }
working-channel = { shelf-1 trunk-module-1 1 }
aps-state = on-working
bridge-status = True
last-switch-time = 0
switch-count = 0
aps-cfg-creation-time = 356537747
number-of-channels = 2
psbf-failure = False
channel-mismatch-failure = False
mode-mismatch-failure = False
fepl-failure = False
recv-psbf-count = 0
```

```
recv-mode-mismatch-count = 0
recv-channel-mismatch-count = 0
recv-fepl-count = 0
extra-traffic-flag = False
protection-mode = 1+1
direction-mode = bidirectional
revertive-mode = revertive
rx-k1-byte-value = 00
rx-k2-byte-value = 05
tx-k1-byte-value = 00
tx-k2-byte-value = 00
```



Note The parameters in this profile have no factory defaults. The Stinger system retrieves the value of each field from its automatic protection switching (APS) system information before it creates the profile and refreshes the profile periodically. The system creates a completely new profile whenever a protection group is activated and deletes it when the corresponding protection group is deactivated.

atm-aal-options

Description A subprofile that enables you to specify the ATM adaptation layer (AAL) type.

Usage Following is a listing of the atm-aal-options subprofile with its default values:

```
[in CONNECTION/":atm-aal-options (new)]
aal-enabled = no
aal-type = aal-0
transmit-sdu-size = 1
receive-sdu-size = 1
```

ATM-ADDR-ALIAS

Description A profile that associates a text alias with an Asynchronous Transfer Mode (ATM) address or portion of an ATM address, up to a maximum of 22 bytes. After you define an alias, you can use the alias in place of the associated numbers in some contexts. The system also displays the alias name in the output of some commands.

Usage Following is a listing of the atm-addr-alias profile with its default settings:

```
[in ATM-ADDR-ALIAS/" (new)]
alias-name* = ""
address = 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
length = 0
```

See Also PNNI-NODE-CONFIG

ATM-CONFIG

Description *Deprecated and not used.*

See Also HIGH-SPEED-SLOT-STATIC-CONFIG
SLOT-STATIC-CONFIG

atm-connect-options

Description A subprofile that enables you to configure options for the second leg of an Asynchronous Transfer Mode (ATM) circuit.

Usage Following is a listing of an `atm-connect-options` subprofile with its default settings:

```
[in CONNECTION/"" : atm-connect-options (new)]  
atm1483type = aal5-llc  
vpi = 0  
vci = 35  
atm-enabled = yes  
nailed-group = 1  
cast-type = p2p  
conn-kind = pvc  
vp-switching = no  
target-atm-address =  
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:  
target-select = required  
target-vpi = 0  
target-vci = 0  
spvc-retry-interval = 10  
spvc-retry-threshold = 1  
spvc-retry-limit = 0  
atm-direct-enabled = no  
atm-direct-profile = ""  
vc-fault-management = none  
vc-max-loopback-cell-loss = 1  
fr-08-mode = translation  
atm-circuit-profile = ""  
oam-ais-f5 = disable  
oam-support = yes  
mtu = 1560
```

ATM-IF-CONFIG

Description A profile that enables you to configure Asynchronous Transfer Mode (ATM) interfaces.

Usage Following is a listing of the atm-if-config profile with its default settings:

```
[in ATM-IF-CONFIG/{ { shelf-1 slot-10 0 } 4 } (new)]
address* = { { shelf-1 slot-10 0 } 4 }
base-config = { 255 8192 8 13 0 0 0.0.0.0 ""
39:84:0f:80:01:bc:72:00:01:1a:dd:9+
extension-config = { atmf-uni-pvc-only other 0 1 5 4 private 255 255 32 +
```

See Also base-config, extension-config

ATM-IF-SIG-PARAMS

Description A profile that enables you to configure Asynchronous Transfer Mode (ATM) interface signaling parameters.

Usage Following is a listing of the atm-if-sig-params profile with its default values:

```
[in ATM-IF-SIG-PARAMS/{ { any-shelf any-slot 0 } 0 } (new)]
address* = { { any-shelf any-slot 0 } 0 }
q2931-options = { 2 1 180000 4000 30000 30000 10000 10000 30000 120000 +
qsaal-options = { 50 4 25 67 1000 0 0 0 15000 no no no }
```

ATM-IF-STAT

Description A read-only profile that indicates information about the state of the physical and logical interfaces.

Usage Read-only. Following is a listing of the atm-if-stat profile with sample settings:

```
[in ATM-IF-STAT/{ { shelf-1 slot-1 20 } 0 }]
address* = { { shelf-1 slot-1 20 } 0 }
if-number = 159
nailed-group = 20
port-state = down
signalling-state = not-configured
pnmi-link-state = not-configured
ilmi-link-state = up
```

ATM-INTERNAL

Description A profile that enables you to configure the Asynchronous Transfer Mode (ATM) internal interface of line interface modules (LIMs) that require an internal interface to terminate ATM traffic, such as router and ISDN digital subscriber line (IDSL) modules.

Usage Following is a listing of the atm-internal profile with its default settings:

```
[in ATM-INTERNAL/{ any-shelf any-slot 0 }]
name = ""
physical-address* = { any-shelf any-slot 0 }
enabled = yes
line-config = { 1 15 }
traffic-shapers = [ { no 1000 1000 2 no 1 } { no 1000 1000 2 no 2 } { no +
```



Note The atm-internal network profile is enabled by default (enabled = yes). If you have previously disabled it, enable it if you intend to use an IDSL module, and save your changes.

ATM-INTERNAL-STAT

Description A profile that provides status parameters of the internal Asynchronous Transfer Mode (ATM) network.

Usage Following are the read-only parameters of the atm-internal-stat profile with typical values:

```
[in ATM-INTERNAL-STAT/{ shelf-1 slot-14 1 }]
physical-address* = { shelf-1 slot-14 1 }
line-state = active
vpi-vci-range = vpi-0-7-vci-32-255
vp-switching-vpi = 15
```

ATM-OAM

Description A profile that enables you to specify operation, administration and management (OAM) F4/F5 support via Simple Network Management Protocol (SNMP).

Usage Following is a listing of the atm-oam profile with its default settings:

```
[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 }
```

Dependencies Consider the following:

- For every virtual path identifier-virtual channel identifier (VPI-VCI) pair for which a test is performed, you must create a separate atm-oam profile.
- When testing multiple circuits using one profile, you can run a loopback test only. One Asynchronous Transfer Mode (ATM) circuit is tested at a time. On each ATM circuit, a specified number of loopback cells are sent, with an interval of one second between each transmission. After the test on one circuit is complete, the unit tests the next circuit.
- Any changes made in an atm-oam profile restart the test. Only that test whose subprofile is changed is restarted.
- While testing one ATM circuit using one profile, loopback and continuity tests can be run concurrently.
- 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.

atm-options

Description A subprofile that enables you to configure options for an Asynchronous Transfer Mode (ATM) terminating connection on the first (incoming) leg of an ATM circuit.

Usage Following is a listing of the atm-options subprofile with its default settings:

```
[in CONNECTION/":atm-options (new)]
atml483type = aal5-llc
vpi = 0
vci = 35
atm-enabled = yes
nailed-group = 1
cast-type = p2p
conn-kind = pvc
vp-switching = no
target-atm-address =
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
target-select = required
target-vpi = 0
target-vci = 0
spvc-retry-interval = 10
spvc-retry-threshold = 1
spvc-retry-limit = 0
atm-direct-enabled = no
atm-direct-profile = ""
vc-fault-management = none
vc-max-loopback-cell-loss = 1
fr-08-mode = translation
atm-circuit-profile = ""
oam-ais-f5 = disable
oam-support = yes
mtu = 1560
```


ATMP

Description A profile that enables you to configure Ascend Tunnel Management Protocol (ATMP) home agent or foreign agent operations, enabling the Stinger unit to operate as a home agent, a foreign agent, or both.

Usage Following is a listing of the atmp profile with its default settings:

```
[in ATMP]
agent-mode = home-agent
agent-type = gateway-home-agent
udp-port = 5150
home-agent-password = ""
atmp-sap-reply = no
retry-timeout = 3
retry-limit = 10
idle-timer = 30
mtu-limit = 0
force-fragmentation = no
atmp-snmp-trap = no
```

Dependencies After configuring this profile, you must reset the system to begin ATMP operations.

atm-parameters

Description A subprofile of the high-speed-slot-static-config and switch-config profiles.

- In the high-speed-slot-static-config profile, the atm-parameters subprofile enables you to set the priority of the Asynchronous Transfer Mode (ATM) cells associated with the line interface module (LIM) or control module.
- In the switch-config profile, the atm-parameters subprofile enables you to set various ATM parameters for an outgoing queue. Each configured queue must be associated with an outgoing port, which is either a control module slot or a trunk port. Each outgoing port can have multiple outgoing queues.

Usage Following are listings of atm-parameters subprofiles:

- In the high-speed-slot-static-config profile:


```
[in HIGH-SPEED-SLOT-STATIC-CONFIG:atm-parameters (new)]
incoming-priority = low-priority
```
- In the switch-config profile:


```
[in SWITCH-CONFIG/tram-18:atm-parameters]
outgoing-queue = [ { yes 1:18:1 { shelf-1 trunk-module-2 1 } yes no no +
outgoing-shaper = [ { 0 1 8000 } { 0 1 8000 } { 0 1 8000 } { 0 1 8000 } { +
```

ATM-PREFIX

Description A profile that enables you to configure an address or a prefix setting explicitly so that the system uses the setting you specify rather than the system-generated default.

Usage Following is a listing of the atm-prefix profile with its default settings:

```
[in ATM-PREFIX/default (new)]
prefix-name* = default
use-short-address = no
pnni-node-prefix = { 13 39:84:0f:80:01:bc:72:00:01:00:00:00:00 }
spvc-address-prefix = { 0 00:00:00:00:00:00:00:00:00:00:00:00 }
svc-address-prefix = { 0 00:00:00:00:00:00:00:00:00:00:00:00 }
```

Dependencies In the atm-prefix profile, when the soft permanent virtual connection (SPVC) and switched virtual connection (SVC) prefix addresses are zero (0), the SPVC prefix and SVC prefix take their values from the PNNI node prefix. Whenever you explicitly configure an address or a prefix setting, the system uses the value you specify rather than the system-generated default. If you delete the atm-prefix profile, the system creates a new one at the next system startup and derives the default prefix from the primary controller serial number.

ATMPVC-STAT

Description A read-only profile that monitors the status of an Asynchronous Transfer Mode (ATM) permanent virtual channel (PVC).

Usage Read-only. Following is sample listing of the atmpvc-stat profile:

```
[in ATMPVC-STAT/unit1]
circuit-name* = unit1
pvc-type = connecting
current-state = pvc-data-transfer
vcc-members = [ { shelf-1 trunk-module-1 1 0 120 801 } { shelf-1 slot-13 12+
magic-keys = [ 0 201326688 ]
```

ATM-QOS

Description A profile that enables you to configure Quality of Service (QoS) settings for an Asynchronous Transfer Mode (ATM) link.

Usage Following is a listing of the atm-qos profile with sample settings:

```
[in ATM-QOS/" (new)]
contract-name* = ""
traffic-descriptor-index = 0
traffic-descriptor-type = noclp-noscr
atm-service-category = cbr
peak-rate-kbits-per-sec = 16
peak-cell-rate-cells-per-sec = 37
sustainable-rate-kbits-per-sec = 16
sustainable-cell-rate-cells-per-sec = 37
minimum-rate-kbits-per-sec = 16
minimum-cell-rate-cells-per-sec = 37
```

```
ignore-cell-delay-variation-tolerance = yes
cell-delay-variation-tolerance = 20
ignore-max-burst-size = yes
max-burst-size = 4
aal-type = aal-0
early-packet-discard = no
partial-packet-discard = no
tag-or-discard = discard
external-change = no
sub-channel = 1
```



Note To disable peak cell rate (PCR) policing, set peak-rate-kbits-per-sec and cell-delay-variation-tolerance values to zero (0).

Dependencies If you attempt to save an atm-qos profile and the traffic-descriptor-type and atm-service category parameters are set to incompatible settings, the Stinger unit generates an error message. Table 2-1 lists the compatible settings for the atm-service category and traffic-descriptor-type parameters.

Table 2-1. Compatible settings for the atm-service-category and traffic-descriptor-type parameters

traffic-descriptor-type parameter	atm-service-category parameter		
Setting	cbr	real-time-vbr or non- real-time-vbr	ubr
noclp-noscr	Valid		Valid
noclp-scr		Valid	
clp-notagging-scr		Valid	
clp-tagging-scr		Valid	
clp-transparent-noscr	Valid		
clp-transparent-scr		Valid	
noclp-tagging-noscr			Valid
noclp-noscr-cdvt	Valid		Valid
noclp-scr-cdvt		Valid	
clp-notagging-scr-cdvt		Valid	
clp-tagging-scr-cdvt		Valid	

atm-qos-options

Description A subprofile that specifies the traffic contract name(s) for the upstream and downstream traffic on the Asynchronous Transfer Mode (ATM) circuit.

Usage Following is a listing of the atm-qos-options subprofile with its default settings:

```
[in CONNECTION/tim:atm-qos-options]
usr-up-stream-contract=""
usr-dn-stream-contract=""
subtending-hops = 0-level
```

ATM-SPVC-ADDR-CONFIG

Description A profile that enables you to configure the address for an Asynchronous Transfer Mode (ATM) soft permanent virtual channel (SPVC).

Usage Following is a listing of the atm-spvc-addr-config profile with its default settings:

```
[in ATM-SPVC-ADDR-CONFIG/{ { shelf-1 slot-1 1 } 0 }]
index* = { { shelf-1 slot-1 1 } 0 }
spvc-atm-address =
39:84:0f:80:01:bc:72:00:01:11:37:93:00:ff:74:09:b7:3d:01:00
external-change = no
```

ATM-SPVC-CONFIG

Description A profile that enables you to configure an Asynchronous Transfer Mode (ATM) soft permanent virtual channel (SPVC).

Usage Following is a listing of the atm-spvc-config profile with its default settings:

```
[in ATM-SPVC-CONFIG (new)]
failure-trap-enable = yes
failure-notification-interval = 30
```

Dependencies This profile only appears on the interface when a corresponding Simple Network Management Protocol (SNMP) MIB table has been entered. The profile disappears from the interface when that MIB table is removed.

ATMVCC-STAT

Description A profile that provides status information about each side of a circuit. The system creates an atmvc-stat profile for each virtual channel connection (VCC) interface.

Usage Following is a listing of an atmvc-stat profile:

```
[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
```

ATM-VCL-CONFIG

Description A profile that enables you to configure an Asynchronous Transfer Mode (ATM) virtual channel link (VCL).

Usage Following is a listing of the atm-vcl-config profile with its default settings:

```
[in ATM-VCL-CONFIG/{ { { any-shelf any-slot 0 } 0 } 0 0 } (new)]
id* = { { { any-shelf any-slot 0 } 0 } 0 0 }
rx-traffic-desc = 1
tx-traffic-desc = 1
aal-type = not-present
tx-sdu-size = 0
rx-sdu-size = 0
aal5-encaps = llc-encapsulation
mcast-type = p2p
call-kind = pvc
```

Dependencies This profile only appears on the interface when a corresponding Simple Network Management Protocol (SNMP) MIB table has been entered. The profile disappears from the interface when that MIB table is removed.

ATM-VPL-CONFIG

Description A profile that enables you to configure an Asynchronous Transfer Mode (ATM) virtual path link (VPL).

Usage Following is a listing of the atm-vpl-config profile with its default settings:

```
[in ATM-VPL-CONFIG/{ { { any-shelf any-slot 0 } 0 } 0 } (new)]
id* = { { { any-shelf any-slot 0 } 0 } 0 }
rx-traffic-desc = 1
tx-traffic-desc = 1
mcast-type = p2p
call-kind = pvc
```

Dependencies This profile only appears on the interface when a corresponding Simple Network Management Protocol (SNMP) MIB table has been entered. The profile disappears from the interface when that MIB table is removed.

See Also id*

auxiliary-syslog [n]

Description The log profile contains two auxiliary-syslog subprofiles. Each syslog data stream is configured independently.

- All the settings in the log profile, except the syslog-format value, affect the first data stream. The syslog-format setting controls the format of all syslog streams.
- The settings in the auxiliary-syslog[1] subprofile affect the second data stream.
- The settings in the auxiliary-syslog[2] subprofile affect the third data stream.

Usage Following is a listing of the auxiliary-syslog[1] subprofile with its default settings:

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

B

bandwidth-config [n]

Description *Deprecated and not used.*

See Also SLOT-STATIC-CONFIG

BANDWIDTH-STATS

Description A read-only profile that provides information about bandwidth allocation for a line interface module (LIM).

Usage Read-only. Following is a listing of the bandwidth-stats profile with sample settings:

```
[in BANDWIDTH-STATS]
max-upstream-bandwidth=622160
active-upstream-bandwidth-on-trunks=155540
standby-upstream-bandwidth-on-trunks=466620
```

BASE

Description A read-only profile that displays the software version, enabled features, network interfaces, and other system information.

Usage Read-only. Following is a listing of a base profile with sample settings:

```
[in BASE]
shelf-number = 1
software-version = 9
software-revision = 3
software-level = ""
manufacturer = dba-ascend-mfg
d-channel-enabled = yes
aim-enabled = no
switched-enabled = yes
multi-rate-enabled = no
t1-pri-conversion-enabled = no
frame-relay-enabled = yes
maxlink-client-enabled = disabled
data-call-enabled = yes
serial-number = 9487770
hardware-level = 0
countries-enabled = 511
domestic-enabled = yes
phs-2-1-support = no
firewalls-enabled = no
network-management-enabled = no
phs-support = no
routing-protocols-disabled = no
tnt-adsl-restricted = yes
tnt-sdsl-restricted = yes
tnt-idsl-restricted = yes
metallic-test-access-unit = no
ss7asg = disabled
atmp-enabled = disabled
l2tp-enabled = disabled
pptp-enabled = disabled
l2f-enabled = disabled
sdtn-enabled = disabled
vrouter-enabled = disabled
v110-enabled = disabled
network-mgmt-voip-enabled = no
wormarq-enabled = disabled
nm-copper-loop-test-enabled = yes
nm-reporting-enabled = no
nm-vpn-enabled = no
nm-navis-radius-enabled = yes
restrict-redundancy-enabled = no
pnni-enabled = yes
ima-enabled = yes
subtended-connections-enabled = no
aps-enabled = yes
nm-prov = yes
```

```
nm-prov-core = no
ras-enabled = no
h248 = no
calea = no
```

base-config

Description A subprofile that enables you to configure bandwidth allocation settings for Asynchronous Transfer Mode (ATM) transmissions

Usage Following is a listing of the base-config subprofile with its default settings:

```
[in ATM-IF-CONFIG/{ { shelf-1 slot-10 0 } 4 }:base-config (new)]
max-vpcs = 255
max-vccs = 8192
max-active-vpi-bits = 8
max-active-vci-bits = 13
ilmi-vpi = 0
ilmi-vci = 0
neighbor-ip-address = 0.0.0.0
neighbor-name = ""
subsc-atm-address = 39:84:0f:80:01:bc:72:
```

bir-options

Description A subprofile for specifying bridged IP routing (BIR) settings.

Usage Specify settings in this subprofile to enable the Stinger unit to establish a connection that uses BIR. Following is a listing of the subprofile with its default settings:

```
[in CONNECTION/":bir-options]
enable = no
proxy-arp = no
multiple-ip-address = { no [ { 0.0.0.0/0 0.0.0.0/0 } { 0.0.0.0/0 0.0.0.0/0 +
```

bootp-relay

Description A subprofile containing options for configuring the BOOTP relay feature. You can enable or disable BOOTP relay and specify a bootp-server address.

Multiple DHCP servers are not supported.

Usage Following is a listing of a bootp-relay subprofile with its default settings:

```
[in IP-GLOBAL:bootp-relay (new)]
active = no
bootp-servers = [ 0.0.0.0 0.0.0.0 ]
relay-agent-information = { { no 0.0.0.0 } {no 0.0.0.0} }
```


bridge-group

Description The index of a bridge-group profile specifies bridging-group number for the VLAN.

Usage Following are the bridge-group parameters, shown with default settings:

```
[in BRIDGE-GROUP/0]
enable = no
bridging-group = 0
mac-entry-age-time = 300
igmp-snooping = no
port-block-enabled = yes
lan-router-interface-address = { { any-shelf any-slot 0 } 0 }
wan-router-interface-profile = ""
```

bridging-options

Description A subprofile of either the connection or ethernet profile that specifies packet bridging settings.

Usage Following is a listing of the CONNECTION/":bridging-options subprofile with its default settings:

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

Following is a listing of the ethernet:briding-options subprofile with its default settings:

```
[in ETHERNET/{ any-shelf any-slot 0 }:bridging-options]
bridging-group = 0
bridge = no
dial-on-broadcast = no
bridge-type = transparent-bridging
vlan-stack-user-vlan-id = 0
qos-interface-group = 0
packet-flows = ""
mac-address-learning-limit = 0
```

Following is a listing of the vlan-ethernet:briding-options subprofile with its default settings:

```
[in VLAN-ETHERNET/{ { shelf-1 first-control-module 2 } 50 }:bridging-options]
bridging-group = 0
bridge = no
dial-on-broadcast = no
```

C

CALL-INFO

Description A read-only profile that provides active call information.

Usage Read-only. Following is a listing of a call-info profile with its default settings:

```
[in CALL-INFO/{ 38 }]
mbid* = { 38 }
call-service = nailed-up
called-number-type = 2
nailed-up-group = 801
call-by-call = 0
phone-number = ""
transit-number = ""
billing-number = ""
switched-call-type = 2
ft1-caller = 0
calling-number = { "" unknown unknown unspecified unspecified }
force-56kbps = 0
redirect-number = ""
call-direction = 1
isdn-signaling = False
```

calling-number

Description A read-only subprofile that indicates active call information about the number that is calling.

Usage Read-only. Following is a listing of the calling-number subprofile with its default settings:

```
[in CALL-INFO/{ 38 }:calling-number]
calling-number = ""
type-of-number = unknown
numbering-plan = unknown
presentation = unspecified
screening = unspecified
```

CALL-LOGGING

Description A profile that enables you to configure the Stinger unit to communicate with one or more call-log hosts. Call logging is a RADIUS-accounting based feature for logging call information from the Stinger unit. Its main purpose is to duplicate accounting information for sites that wish to keep accounting records separate from call-logging details used to manage resources or troubleshoot call problems.

Once you have configured call logging, the Stinger unit sends Start session, Stop session, and Failure-to-Start session packets to a call-log host. A call-log host is a local host that supports the RADIUS accounting protocol and is configured properly to communicate with the Stinger unit (for example, a RADIUS accounting server or a host running NavisAccess). The call-log information is sent independently of RADIUS accounting records. If both call logging and RADIUS accounting are in use, the information is sent in parallel.

Usage Following is a listing of the call-logging profile with its default settings:

```
[in CALL-LOGGING (new)]
call-log-enable = no
call-log-host-1 = 0.0.0.0
call-log-host-2 = 0.0.0.0
call-log-host-3 = 0.0.0.0
call-log-port = 1646
call-log-key = ""
call-log-timeout = 1
call-log-id-base = acct-base-10
call-log-reset-time = 0
call-log-stop-only = yes
call-log-limit-retry = 0
call-log-server-index = host-1
call-log-evaluation-end-julian-time = 0
call-log-radius-compatible = 16-bit-vendor-specific
call-log-multi-packet = no
call-log-stream-period = 15
call-log-connection-packets-enable = no
call-log-csm-modem-diag = no
```

CALL-ROUTE

Description A profile that the Stinger unit uses to control the routing of incoming and outgoing calls. Every possible destination within a system has one or more profiles of this type.

Usage Following is a listing of the call-route profile with sample settings:

```
[in CALL-ROUTE/{ { { shelf-1 any-slot 0 } 0 } 0 }]
index* = { { { shelf-1 any-slot 0 } 0 } 0 }
trunk-group = 0
phone-number = ""
preferred-source = { { any-shelf any-slot 0 } 0 }
call-route-type = any-call-type
```

CARD-CODE

Description *Not used.* A read-only profile that displays the enabled features on a module.

channel-config[n]

Description A subprofile that enables you to configure each logical link associated with an ISDN digital subscriber line (ISDL).

Usage Following is a listing of a channel-config subprofile with its default settings:

```
[in ISDL/{ shelf-1 slot-13 1 }:line-interface:channel-config[1]]
spid = ""
phone-number = ""
trunk-group = 0
channel-usage = switched-channel
route-port = { { 0 0 } { 0 } }
call-route-info = { any-shelf any-slot 0 }
nailed-group = 605
```

channel-state

Description A read-only subprofile that displays the state of each of the two ISDN digital subscriber line (ISDL) channels.

Usage Read-only. Following is a listing of a channel-state subprofile with its default settings:

```
[in ISDL-STAT/{ shelf-1 slot-13 1 }:channel-state]
channel-state[1] = disabled
channel-state[2] = disabled
```

circuit-id

Description A subprofile that enables you to configure settings for the circuit identifier suboption of DHCP option 82.

Usage Following is a listing of the circuit-id subprofile with its default settings:

```
[in IP-GLOBAL:bootp-relay:relay-agent-information:circuit-id]
enable = no
if-ip = 0.0.0.0
version = 1
dhcp-allow-any-src-port = no

[in BRIDGE-GROUP/0:dhcp-snooping:circuit-id (new)]
enable = no
if-ip = 0.0.0.0
vendor-option-string = ""
version = 1
dhcp-allow-any-src-port = no
```

```
[in BRIDGE-GROUP/0:pppoe-snooping:circuit-id (new)]
enable = no
if-ip = 0.0.0.0
vendor-option-string = ""
version = 1
dhcp-allow-any-src-port = no
```

CLT-ACCESS

Description *Deprecated and not used.*

See Also CLT-MS-ACCESS

CLT-COMMAND

Description A profile that enables you to configure the parameters required to run any of the tests provided by the copper loop test (CLT) module. The `test-operation` parameter defines the test to be performed. Any change to the value of this parameter initiates the test identified by the new value.



Note The `test-operation` parameter should be set after all the other parameters for the desired test are configured.

Usage Following is a listing of the `clt-command` profile with sample settings:

```
[in CLT-COMMAND (new)]
cltm-slot = slot-16
test-time-stamp = 0
test-sequence = 0
test-operation = none
dmm-type = resistance
dmm-lead = tip-ring
background-noise-filter = psd
background-noise-termination = term100
loop-resistance-unit = metric
loop-resistance-temp = 0
impulse-noise-start-thresh = 50
impulse-noise-start-delta = 2
impulse-noise-start-max-count = 1
impulse-noise-start-dead-time = 1
impulse-noise-start-timer = 1
calibration-type = insertion-loss
tone-send-freq = 10
tone-send-level = 0
tone-send-period = 0
tdr-unit = metric
tdr-gauge = 0
tdr-vp = 0
tdr-avg = 1
tdr-get-type = automatic
tdr-start-distance = 0
tdr-measurement-length = 0
dmmddcd-period = 0
```

```
dmddcd-voltage = 0
dmddcd-impedance = 10
dmcap-period = 0
dmall-type = resistance
dmall-period = 0
dmall-input-imp = 0
ctone-type = adsl
ctone-tone = quiet
ttone-lead = tip-ring
ttone-level = 0
ttone-period = 0
btap-start-length = 0
btap-measure-length = 0
fciloc-unit = metric
fciloc-gauge = 0
shortloc-unit = metric
shortloc-gauge = 0
shortloc-type = detect
setresp-mode = on
setresp-mode-period = 0
```

CLT-MS-ACCESS

Description An indexed profile that enables you to configure and activate access to the copper loop test (CLT).

Usage Following is a listing of the `clt-ms-access` profile with its default settings:

```
[in CLT-MS-ACCESS]
cltm-shelf = shelf-2
cltm-slot = slot-3
access-slot = slot-1
access-port = 1
access-loop = 1
access-mode = looking-out
access-terminal = internal-tester-terminal
activate-access = no
access-result = idle
access-timeout = 5
```

CLT-MS-ACCESS-STAT

Description Displays the status of the copper loop test (CLT) access.

Usage Following is a listing of the `clt-ms-access-stat` profile with its default settings:

```
[in CLT-MS-ACCESS-STAT/shelf-1]
cltm-shelf* = shelf-1
access-result = idle
access-start-time = { 0 0 0 }
access-start-date = { Monday January 1990 1 }
access-end-time = { 0 0 0 }
access-end-date = { Monday January 1990 1 }
access-change-reason = deactivation
```

CLT-RESULT

Description A profile that indicates the test result of all the tests the tester module has executed. The `test-result-status` parameter is set to `not-valid` at the start of each test and is updated to `valid` or `out-of-range` at the end of each test. All of the `clt-result` profile is cleared at the start of each test, and, depending on the test, the corresponding result parameters are updated at the end.

Usage Following is a listing of a `clt-result` profile with sample settings:

```
[in CLT-RESULT (new)]
cltm-slot = slot-16
test-result-time-stamp = 0
test-result-sequence = 0
test-result-status = not-ready
dmm-result = 0
loop-resistance = 0
loop-resistance-length-1 = 0
loop-resistance-length-2 = 0
loop-resistance-length-3 = 0
coil-detection-coil-count = 0
impulse-noise-read-low-threshold = 0
impulse-noise-read-mid-threshold = 0
impulse-noise-read-high-threshold = 0
rcv-tone-frequency = 0
rcv-tone-level = 0
tdr-manual-sample-count = 0
tdr-automatic-fault-distance = 0
hardware-revision = 0
software-revision = 0
psd-frequency-level = [ { 0 0 } { 0 0 } { 0 0 } { 0 0 } { 0 0 } { 0 0 } { 0 0 }
tdr-distance-level = [ { 0 0 } { 0 0 } { 0 0 } { 0 0 } { 0 0 } { 0 0 } { 0 0 }
dc-delta-resistance-t-r = 0
dc-delta-resistance-t-s = 0
dc-delta-resistance-r-s = 0
dc-delta-voltage-t-s = 0
dc-delta-voltage-r-s = 0
cap-equivalent-t-r = 0
```

```
cap-equivalent-t-s = 0
cap-equivalent-r-s = 0
dmm-all-t-r = 0
dmm-all-t-s = 0
dmm-all-r-s = 0
ringer = 0
atu-r = 0
bridge-tap-number = 0
bridge-tap-length = 0
bridge-tap-table = [ { 0 0 0 } { 0 0 0 } { 0 0 0 } { 0 0 0 } { 0 0 0 } { 0 0 +
voice-detection = 0
first-coil-location = 0
short-location = 0
splitter-det-result = 0
```

cmd-log

Description The cmd-log profile contains read-only parameters that provide details about a logged command entry. If this feature is enabled, the system creates a cmd-log profile for every command entered by a user.

Usage Following is a listing of a sample cmd-log profile with an index number of 92:

```
[in CMD-LOG/92]
user = admin
session-id = 2
login-source = console
log-date = { Friday November 2003 7 }
log-time = { 6 58 12 }
information = "dir cmd-log"
index* = 92
shelf = 1
slot = 9
```

CONNECTION

Description A profile that enables you to configure connection-specific information, including user-password authentication settings, compression values, filter specifications, and Asynchronous Transfer Mode (ATM) options.

Usage Following is a listing of the connection profile with its default settings:

```
[in CONNECTION/"" ]
station* = ""
active = no
encapsulation-protocol = atm-circuit
called-number-type = national
dial-number = ""
clid = ""
auto-profiles = yes
ip-options = { yes yes 0.0.0.0/0 0.0.0.0/0 1 60 120 no 0 0.0.0.0 +
bridging-options = { 0 no no }
session-options = { "" "" no 120 no-idle 120 "" 0 disabled autobaud+
```



```
telco-options = { ans-and-orig no ft1 1 no no 56k-clear 0 "" "" no +
ppp-options = { no-ppp-auth none "" none "" "" "" "" stac 1524 no 6+
mp-options = { 1 1 2 }
mpp-options = { "" quadratic transmit 1 1 15 5 10 70 }
fr-options = { "" 16 "" transparent-link no "" 16 "" }
tcp-clear-options = { "" 0 "" 0 "" 0 "" 0 no "" 256 20 }
usrRad-options = { global 0.0.0.0 1646 "" 1 acct-base-10 }
calledNumber = ""
shared-prof = no
max-shared-users = 0
tunnel-options = { disabled atmp-protocol 0 rip-off "" "" 5150 "" "+"
vrouter = ""
cross-connect-index = 0
atm-options = { aal5-llc 0 35 1 p2p pvc no 00:00:00:00:00:00:00:00:+
atm-connect-options = { aal5-llc 0 35 1 p2p pvc no 00:00:00:00:00:00:00:0+
port-redirect-options = { none 0 0.0.0.0 }
pppoe-options = { no no }
atm-qos-options = { default default 0-level }
bir-options = { no no }
atm-aal-options = { no aal-0 1 1 }
conn-user = default
```

Dependencies The following connection profile entries do not apply to Stinger units:

```
called-number-type = national
dial-number = ""
clid = ""
expect-callback = no
mp-options = { 1 1 2 }
mpp-options = { "" quadratic transmit 1 1 15 5 10 70 }
tcp-clear-options = { "" 0 "" 0 "" 0 "" 0 no "" 256 20 }
calledNumber = ""
```

contact-closure

Description The contact-closure subprofile indicates the contact closure state of the corresponding remote shelf. This profile is read-only.

Usage Following are the read-only fields in a profile for shelf 2:

```
[in REMOTE-SHELF-STAT/shelf-2:contact-closure]
contact-closure[1] = no
contact-closure[2] = no
contact-closure[3] = no
contact-closure[4] = no
contact-closure[5] = no
contact-closure[6] = no
contact-closure[7] = no
```



Note Only the first two contact closure values are meaningful for Stinger MRT units.

context [n]

Description A subprofile that enables you to configure options for an individual controller. The index for each subprofile is a controller number.

Usage Following is a listing of the context [n] subprofile with its default setting:

```
[in REDUNDANCY:context [1]]
must-agree=no
```

context-stats [n]

Description A subprofile that contains the redundancy statistics for a particular control module. There is one context-stats subprofile for each control module.

Usage Following are the read-only parameters in the context-stats subprofile:

```
[in REDUNDANCY-STATS:context-stats [1]]
state = monitoring
function = secondary
select-reason = defer-to-running-primary
prior-function = secondary
last-reboot = crash
local = { 9487770 }
pair = { 10486893 }
chassis-serial-number = 0
initialization-time = 382400025
post-start = 382400029
post-end = 382400031
selection-start = 382400029
selection-end = 382400031
load-start = 382400031
load-end = 382400074
inauguration-time = 382400074
last-sent = 382400074
last-received = 382400074
last-profile-sync = 0
last-code-sync = 0
last-log-recv = 0
update-time = 382400074
```

continuity-config

Description A subprofile that you use to configure continuity check parameters.

Usage Set values in this profile to specify the continuity check parameters. Following is a listing of continuity-config subprofile with its default settings:

```
[in ATM-OAM/{ { any-shelf any-slot 0 } 0 0 }:continuity-config (new)]
enabled = no
continuity-level = segment
```

controller-static-config

Description *Deprecated and not used.*

See Also switch-config

D

date

Description A subprofile that enables you to configure the day of the week and the current system date.

Usage Following is a listing of the date subprofile with sample settings:

```
[in TIMEDATE:date]
weekday=Friday
month=October
day=18
year=1996
```



Note You can also use the date command to set the day of the week and the system date.

DEBUG

Description A profile that enables you to configure Stinger debug options.

Usage Following is a listing of the debug profile with its default settings:

```
[in DEBUG/{ any-shelf any-slot 0 }]
physical-Address* = { any-shelf any-slot 0 }
active = yes
enable-core-dump = no
core-dump-server = ""
enable-gdb = no
gdb-host = ""
generic-field = 2147483647
min-warning-core-dump = 0
max-warning-core-dump = 0
core-dump-rip-update = update-high-freq
```

device-address

Description A subprofile that enables you to configure the address for the device carrying the call.

Usage Following is a listing for the device-address subprofile with its default settings:

```
[in CALL-ROUTE/{ { { shelf-1 any-slot 0 } 0 } 0 } :index:device-address]
physical-address = { shelf-1 any-slot 0 }
logical-item = 0
```

See Also index, preferred-source

DEVICE-STATE

Description A read-only profile that indicates the current state of a device. The Stinger unit does not store the device-state profile in nonvolatile RAM (NVRAM), so the profile's settings do not persist across system resets or power cycles. The device-state parameter setting might differ from the reqd-state parameter setting during state changes, such as when a device is being disconnected. State changes are complete when the device-state and the reqd-state values match.

Usage Read-only. Following is a listing of the device-state profile with sample settings:

```
[in DEVICE-STATE/{ { { shelf-1 slot-13 19 } 0 } }]
device-address* = { { { shelf-1 slot-13 19 } 0 } }
device-state = down-dev-state
up-status = idle-up-status
reqd-state = down-reqd-state
route-id = { 0 }
used-count = 0
bad-count = 0
last-32 = 0
```

Dependencies A Simple Network Management Protocol (SNMP) manager can read the device-state profile.

dhcp-snooping

Description The dhcp-snooping subprofile configures the system to snoop client-to-server DHCP request packets and add identifiers before bridging the packets upstream.

Usage Following is a listing of the dhcp-snooping profile with its default settings:

```
[in BRIDGE-GROUP/0:dhcp-snooping (new)]
enable = no
circuit-id = { no 0.0.0.0 "" 1 no }
remote-id = { no 0.0.0.0 "" 1 no }
```

dialout-configuration

Description *Not used.*

Location `TERMINAL-SERVER`

dialout-options

Description *Not supported.* A `tunnel-server` subprofile that specifies dial-out options for a specific Layer 2 Tunneling Protocol (L2TP) network server (LNS). The parameters in this subprofile do not apply to Stinger units operating as L2TP access concentrators (LACs).

Location `TUNNEL-SERVER`

dlci-ident

Description A read-only subprofile that indicates data link connection identifier (DLCI) information.

Usage Read only. Following is a listing of a `dlci-ident` subprofile with sample settings:

```
[in FRDLCI-STAT/{ 16 3 fr13_20_1 transparent-link }:dlci-ident]
dlci = 16
dlci-route-id = 3
fr-profile = fr13_20_1
fr-link-type = transparent-link
```

dlci-members [n]

Description A read-only subprofile that indicates the data link connection identifier (DLCI) information for each of the DLCI members.

Usage Read-only. Following is a sample listing of the `dlci-members` subprofile:

```
[in FRPVC-STAT/801_0_120:dlci-members[1]]
dlci = 16
dlci-route-id = 3
fr-profile = fr13_20_1
fr-link-type = transparent-link
```

dns-local-table

Description A subprofile that enables you to configure a Domain Name System (DNS) table of up to eight hostnames and their IP addresses. The system consults the table in RAM for address resolution only if requests to the DNS server fail. The local table acts as a safeguard to ensure that the system can resolve certain DNS names, even if all DNS servers are inaccessible.

The local DNS table is propagated to RAM from the settings in this subprofile. At startup, the system copies values in the profile to the table in RAM. If you subsequently modify the `dns-local-table` subprofile, the changes are propagated to the table in RAM when the profile is written.

Usage Following is a listing of the dns-local-table subprofile with its default settings:

```
[in IP-GLOBAL:dns-local-table]
enabled = no
auto-update = no
table-config = [ { "" 0.0.0.0 } { "" 0.0.0.0 } { "" 0.0.0.0 } { "" 0.+
```

See Also table-config

DS1-ATM

Description A profile that enables you to configure hardware-specific parameters that are common to the inverse multiplexing over ATM (IMA) chip. For example, because 24-port IMA line interface modules (LIMs) contain three chips, three profiles are created. However, because eight-port IMA LIMs contain a single chip, only one profile is created.

Usage Following is a listing of ds1-atm profile with its default settings:

```
[in DS1-ATM/{ any-shelf any-slot 0 } (new)]
name = 0:0:0
physical-address* = { any-shelf any-slot 0 }
enabled = no
spare-physical-address = { any-shelf any-slot 0 }
sparing-mode = inactive
ignore-lineup = system-defined
line-config = { esf b8zs 4294967246 no-loopback not-eligible high-priority +
```

DS1-ATM-STAT

Description A read-only profile that indicates the statistics for DS1-ATM modules.

Usage Read-only. Following is a sample listing of a ds1-atm-stat profile:

```
[in DS1-ATM-STAT/{ shelf-1 slot-2 1 }]
physical-address* = { shelf-1 slot-2 1 }
line-mode = uni
line-state = disabled
loss-of-carrier = True
loss-of-sync = False
ais-receive = True
yellow-receive = False
ber-receive = False
carrier-established = False
cell-delineation = False
network-loopback = False
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 +
```

```
ima-link-statistic = { 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 }
utopia-address = 4294967295
send-code-status = disabled
pattern-test-status = none
```

DS3-ATM

Description A profile that enables you to configure a DS3-ATM module.

Usage Following is a listing of the ds3-atm profile with its default settings:

```
[in DS3-ATM/{ shelf-1 slot-1 0 }]
name=""
physical-address*={ shelf-1 slot-1 0 }
enabled=no
spare-physical-address={ any-shelf any-slot 0 }
sparing-mode=inactive
ignore-lineup = system-defined
line-config={ 9 0 static { shelf-1 slot-1 0 } no-loopback no +
```

DS3-ATM-STAT

Description A read-only profile that indicates the status of a DS3-ATM trunk module.

Usage Read-only. Following is a sample listing of the ds3-atm-stat profile:

```
[in DS3-ATM-STAT/{ shelf-1 trunk-module-2 1 }]
physical-address* = { shelf-1 trunk-module-2 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-32-4095
vc-switching-vpi = "0 10 20 30 40 50"
vcc-vpi = [ 0 0 0 0 0 0 0 0 0 0 0 0 10 0 0 0 0 0 0 0 0 0 0 0 20 0 0 0 0 0 0 0 0 0 0 30+
f-bit-error-count = 227
p-bit-error-count = 9
cp-bit-error-count = 5
feb-error-count = 24
bpv-error-count = 5303
loss-of-signal = False
loss-of-frame = False
yellow-receive = False
ais-receive = False
```

DSL-THRESHOLD

Description A profile that enables you to configure threshold settings for digital subscriber line (DSL) services.

Usage Following is a listing of the `dsl-threshold` profile with its default settings:

```
[in DSL-THRESHOLD/default]
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
```


E

E3-ATM

Description A profile that enables you to configure the parameters for an E3 trunk module.

Usage Following is a listing of the e3-atm profile with its default values:

```
[in E3-ATM/{ any-shelf any-slot 0 } (new)]
name = ""
physical-address* = { any-shelf any-slot 0 }
enabled = no
ignore-lineup = system-defined
line-config = { 9 1 no-loopback no g832-adm vpi-0-255-vci-32-8191 [ 0 0 0 0+
spare-physical-address = { any-shelf any-slot 0 }
sparing-mode = inactive
```

E3-ATM-STAT

Description A read-only profile that indicates the status of a E3-ATM trunk module.

Usage Read-only. Following is a sample listing of the e3-atm-stat profile:

```
[in E3-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 = "0 10 20 30 40 50"
vcc-vpi = [ 0 0 0 0 0 0 0 0 0 0 0 10 0 0 0 0 0 0 0 0 0 20 0 0 0 0 0 0 0 0 30+
f-bit-error-count = 0
p-bit-error-count = 0
cp-bit-error-count = 0
feb-error-count = 0
bpv-error-count = 0
loss-of-signal = False
loss-of-frame = False
yellow-receive = False
ais-receive = False
```

ERROR

Description A read-only profile that provides information about any errors that occur when the Stinger unit is running.

Usage Read-only. Following is a sample listing of the error profile:

```
[in ERROR/562]
is-post = no
type = 99
abstime = 380755993
slot = 9
version = 9.0-169a0e0
user-profile = admin
stack-trace = [ 0 0 0 0 0 0 ]
loadname = stngrcm
index* = 562
shelf = 1
login-source = 192.168.120.10
```

ETHER-INFO

Description A read-only profile that indicates the Media Access Control (MAC) address and link state of an Ethernet interface. The ether-info profile is created when the Ethernet module enters an active state and deleted when the slot is deactivated. The contents of the profile are not written to nonvolatile RAM (NVRAM).

Usage Read-only. Following is a listing of the ether-info profile with sample settings:

```
[in ETHER-INFO/{ shelf-1 slot-2 1 }]
interface-address*={ shelf-1 slot-2 1 }
mac-address=00:c0:7b:68:ef:98
link-state=up
media-speed-mbit = 100
```

ETHERNET

Description A profile that enables you to configure the physical characteristics of an Ethernet interface. With the optional line element module (LEM) of a router module, two additional Ethernet interfaces are supported by the Stinger unit.

Usage Following is a listing of the ethernet profile with its default settings:

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

ethernet-filter

Description Filters input streams on the basis of Ethernet type and MAC addresses.

Usage Following is a listing of the ethernet-filter subprofile shown with default settings:

```
[in FILTER/"" :input-filters[1]:ethernet-filter]
source-mac-address = 00:00:00:00:00:00
destination-mac-address = 00:00:00:00:00:00
ethernet-type = 00:00
```

extension-config

Description A subprofile containing supplemental parameters for configuring the Asynchronous Transfer Mode (ATM) cell layer.

Usage Following is a listing of the extension-config subprofile with its default settings:

```
[in ATM-IF-CONFIG/{ { any-shelf any-slot 0 } 0 } :extension-config (new)]
config-type = atmf-uni-pvc-only
config-side = other
ilmi-admin-status = no
ilmi-connectivity = no
conn-estab-interval = 1
loss-detect-interval = 5
poll-inact-factor = 4
device-type = private
max-switched-vpc-vpi = 255
max-switched-vcc-vpi = 255
min-switched-vcc-vci = 32
sig-vcc-rx-qos-name = default-ctl
sig-vcc-tx-qos-name = default-ctl
pvc-failure-trap-enabled = no
pvc-failure-intvl = 30
```

EXTERNAL-AUTH

Description A profile that enables you to configure options for an external RADIUS server.

Usage Following is a listing of the external-auth profile with sample settings:

```
[in EXTERNAL-AUTH (new)]
auth-type = None
acct-type = none
rad-serv-enable = no
rad-auth-client = { 0.0.0.0 0.0.0.0 0.0.0.0 0 0 "" no 1 no no no 0 yes yes 0+
rad-acct-client = { 0.0.0.0 0.0.0.0 0.0.0.0 0 0 "" 1 0 acct-base-10 all-ses+
rad-auth-server = { 0 no rad-serv-attr-any [ 0.0.0.0 0.0.0.0 0.0.0.0 0.0 0.+
tac-auth-client = { 0.0.0.0 0.0.0.0 0.0.0.0 0 0 "" 0 }
tacplus-auth-client = { 0.0.0.0 0.0.0.0 0.0.0.0 0 0 "" 0 0 }
tacplus-acct-client = { 0.0.0.0 0.0.0.0 0.0.0.0 0 0 "" }
```

```
password-profile = { "" "" ***** ***** ***** ***** ***** }
local-profiles-first = lpf=yes
noattr6-use-termsrv = yes
cli-user-auth = local-then-external
```

F

fast-path-config

Description A subprofile that enables you to configure minimum, maximum, and planned upstream and downstream bit rates for a rate-adaptive connection on a fast channel.

Usage Following is a listing of the fast-path-config subprofile with sample settings:

```
[in AL-DMT/{ shelf-1 slot-4 1 }:fast-path-config]
min-bitrate-up=10
min-bitrate-down=50
max-bitrate-up=1000
max-bitrate-down=8000
planned-bitrate-up=200
planned-bitrate-down=200
```

FILTER

Description A profile that specifies input and output filter specifications.

Usage Values set in this profile can be applied to any number of connection or RADIUS profiles. Following is a listing of the filter profile with its default settings:

```
[in FILTER/""]
filter-name* = ""
input-filters = [ { no no generic-filter { 0 0 no no 00:00:00:00:00:0+
output-filters = [ { no no generic-filter { 0 0 no no 00:00:00:00:00:0+
```

filter-list [n]

Description A subprofile containing a multicast group address. At least 1008 filter-list subprofiles can be specified.

Usage Following is a listing of a filter-list subprofile with its default values:

```
[in MCAST-SERVICE/"":filter-list [1] (new)]
active = no
mcast-ip-address = 0.0.0.0
group-range-count = 1
```

flow

Description An array of 32 indexed subprofiles for classifying and prioritizing for up to 32 packet flows, including the default packet flow which consists of all packets that do not match one of the configured rules.

Usage Following is a listing of the flow subprofile shown with default settings:

```
[in PACKET-FLOWS/":flow (new)]
flow[1] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }
flow[2] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }
flow[3] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }
flow[4] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }
flow[5] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }
flow[6] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }
flow[7] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }
flow[8] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }
flow[9] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }
flow[10] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[11] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[12] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[13] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[14] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[15] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[16] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[17] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[18] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[19] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[20] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[21] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[22] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[23] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[24] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[25] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[26] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[27] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[28] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[29] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[30] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[31] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
flow[32] = { { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } }+
```

flow[n]

Description An array of 32 indexed subprofiles for configuring classification rules and a scheduling priority for up to 32 different flows.

Usage Following is a listing of the flow subprofile shown with default settings:

```
[in PACKET-FLOWS/":flow[1] (new)]
layer2-classifier = { 0 0 00:00 }
packet-classifier = { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 }
scheduling = { 0 }
```

flow-list

Description An array of 32 indexed subprofiles used to configure a set of flow classification rules and corresponding service parameters applicable to those flows.

Usage Following is a listing of the flow-list profile shown with default settings:

```
[in FLOW-SERVICES/"" :flow-list (new)]
flow-list [1] = { { 0 0 00:00 } { 0 } }
flow-list [2] = { { 0 0 00:00 } { 0 } }
flow-list [3] = { { 0 0 00:00 } { 0 } }
flow-list [4] = { { 0 0 00:00 } { 0 } }
flow-list [5] = { { 0 0 00:00 } { 0 } }
flow-list [6] = { { 0 0 00:00 } { 0 } }
flow-list [7] = { { 0 0 00:00 } { 0 } }
flow-list [8] = { { 0 0 00:00 } { 0 } }
flow-list [9] = { { 0 0 00:00 } { 0 } }
flow-list [10] = { { 0 0 00:00 } { 0 } }
flow-list [11] = { { 0 0 00:00 } { 0 } }
flow-list [12] = { { 0 0 00:00 } { 0 } }
flow-list [13] = { { 0 0 00:00 } { 0 } }
flow-list [14] = { { 0 0 00:00 } { 0 } }
flow-list [15] = { { 0 0 00:00 } { 0 } }
flow-list [16] = { { 0 0 00:00 } { 0 } }
flow-list [17] = { { 0 0 00:00 } { 0 } }
flow-list [18] = { { 0 0 00:00 } { 0 } }
flow-list [19] = { { 0 0 00:00 } { 0 } }
flow-list [20] = { { 0 0 00:00 } { 0 } }
flow-list [21] = { { 0 0 00:00 } { 0 } }
flow-list [22] = { { 0 0 00:00 } { 0 } }
flow-list [23] = { { 0 0 00:00 } { 0 } }
flow-list [24] = { { 0 0 00:00 } { 0 } }
flow-list [25] = { { 0 0 00:00 } { 0 } }
flow-list [26] = { { 0 0 00:00 } { 0 } }
flow-list [27] = { { 0 0 00:00 } { 0 } }
flow-list [28] = { { 0 0 00:00 } { 0 } }
flow-list [29] = { { 0 0 00:00 } { 0 } }
flow-list [30] = { { 0 0 00:00 } { 0 } }
flow-list [31] = { { 0 0 00:00 } { 0 } }
flow-list [32] = { { 0 0 00:00 } { 0 } }
```

flow-services

Description Defines the mapping between enterprise VLAN IDs in inbound traffic and NSP VLAN user IDs for outbound traffic on the Gigabit Ethernet port.

Usage Following is a listing of the flow-services profile shown with default settings:

```
[in FLOW-SERVICES/"" (new)]
name* = ""
service-type = none
flow-list = [ { { 0 0 00:00 } { 0 } } { { 0 0 00:00 } { 0 } } { { 0 0 00:00 } +
```

FRAME-RELAY

Description A profile that enables you to configure frame relay connections.

Usage Following is a listing of the frame-relay profile with its default settings:

```
[in FRAME-RELAY/""]  
fr-name* = ""  
active = no  
nailed-up-group = 1  
nailed-mode = ft1  
called-number-type = 2  
switched-call-type = 56k-clear  
phone-number = ""  
billing-number = ""  
transit-number = ""  
call-by-call-id = 0  
link-mgmt = none  
link-type = dte  
n391-val = 6  
n392-val = 3  
n393-val = 4  
t391-val = 10  
t392-val = 15  
MRU = 1532  
dceN392-val = 3  
dceN393-val = 4  
link-mgmt-dlci = dlci0  
mfr-bundle-name = ""  
frf5-options = { no 0 35 16 }
```

Dependencies The frf5-options subprofile is not supported for the IDSL line interface module (LIM).

frame-relay-options

Description A subprofile that specifies the options to match the frame-relay profile when configuring an ISDN digital subscriber line (IDSL) to frame relay connection.

Usage Following is an example of a frame-relay-options subprofile with its default settings:

```
[in CONNECTION/""]  
frame-relay-profile = ""  
dlci = 16  
circuit-name = ""  
fr-link-type = transparent-link  
fr-direct-enabled = no  
fr-direct-profile = ""  
fr-direct-dlci = 16  
mfr-bundle-name = ""  
fr-enabled = yes
```

fr-answer

Description A subprofile that enables the Stinger unit to answer incoming connections that use frame relay encapsulation.

Usage Following is a listing of an fr-answer subprofile with its default setting:

```
[in ANSWER-DEFAULTS:fr-answer (new)]
enabled = yes
```

FRDLCI-STAT

Description This read-only profile that indicates the state of the frame relay data link connection identifier (DLCI) for the permanent virtual channel (PVC).

Usage Read-only. Following is a listing of the frdlci-stat profile with sample settings:

```
[in FRDLCI-STAT/{ 16 3 fr13_20_1 transparent-link }]
dlci-ident* = { 16 3 fr13_20_1 transparent-link }
circuit-name = 801_0_120
current-state = pvc-data-transfer
tag = 4225504
shelf-number = shelf-1
slot-number = slot-13
```

fr-options

Description A subprofile that specifies the options to match the frame-relay profile when configuring an ISDN digital subscriber line (IDSL) to frame relay connection.

Usage Following is a listing of the fr-options subprofile with its default settings:

```
[in CONNECTION/":fr-options (new)]
frame-relay-profile = ""
dlci = 16
circuit-name = ""
fr-link-type = transparent-link
fr-direct-enabled = no
fr-direct-profile = ""
fr-direct-dlci = 16
mfr-bundle-name = ""
fr-enabled = yes
```

Dependencies Frame relay calls must be enabled in the answer-defaults profile.

FRPVC-STAT

Description This read-only profile that displays the state of the frame relay permanent virtual connection (PVC).

Usage Read-only. Following is a listing of the frpvc-stat profile with sample settings:

```
[in FRPVC-STAT/801_0_120]
circuit-name* = 801_0_120
current-state = pvc-data-transfer
transparentPvc = yes
trunkLinkIndex = 0
activeLinkCount = 3
dlci-members = [ { 16 3 fr13_20_1 transparent-link } { 17 4 f _20 transpare+
```

G

gen-filter

Description A subprofile for defining a generic packet filter.

Usage Set values in this subprofile to configure one of up to 12 input or output generic packet filters. Following are listings of gen-filter subprofiles:

- For input filters:


```
[in FILTER/":input-filters[1]:gen-filter]
offset = 0
len = 0
more = no
comp-neq = no
mask = 00:00:00:00:00:00:00:00:00:00:00
value = 00:00:00:00:00:00:00:00:00:00:00
```
- For output filters:


```
[in FILTER/":output-filters[1]:gen-filter]
offset = 0
len = 0
more = no
comp-neq = no
mask = 00:00:00:00:00:00:00:00:00:00:00
value = 00:00:00:00:00:00:00:00:00:00:00
```

H

HDSL2

Description A profile that enables you to configure HDSL2 ports.

Usage Following is a listing of the hds12 profile with its default settings:

```
[in HDSL2/{ any-shelf any-slot 0 } (new)]
name = ""
physical-address* = { any-shelf any-slot 0 }
enabled = no
sparing-mode = inactive
ignore-lineup = system-defined
line-config = { 0 1 15 static { any-shelf any-slot 0 } coe no not-eligible +
thresh-profiles = { DEFVAL "" "" [ { "" "" } { "" "" } { "" "" } { "" "" } +
```

HDSL2-STAT

Description A read-only profile that indicates the status of each HDSL2 interface. The Stinger unit creates an hds12-stat profile for each HDSL2 interface in the system.

Usage Following is a listing of the hds12 profile with sample settings for an active line:

```
[in HDSL2-STAT/{ shelf-1 slot-2 10 }]
physical-address* = { shelf-1 slot-2 10 }
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 = { 0 cpe port-up 1544000 A100 1 }
physical-statistic = { { 0 0 3 } yes 36 3 passed 10 0 in-sync 0 0 0 0 0 0 +
```

HIGH-SPEED-SLOT-STATIC-CONFIG

Description A profile that enables you to configure auxiliary Asynchronous Transfer Mode (ATM) parameters for each trunk or trunk aggregation module (TRAM).

Usage Following is a listing of the high-speed-slot-static-config profile with its default settings:

```
[in HIGH-SPEED-SLOT-STATIC-CONFIG/{ shelf-1 trunk-module-1 1 }]  
name = ""  
physical-address* = { shelf-1 trunk-module-1 1 }  
atm-parameters = { low-priority }  
trunk-cac-config = { yes "" 148598 10 }
```

Dependencies The trunk-cac-config profile was previously located in the atm-config profile. Its use in that location has been deprecated.

If a user has already set this profile in the atm-config profile under a previous TAOS release, the parameters are copied into the corresponding high-speed-slot-static-config profile. The parameters are now invisible in the atm-config profile unless allow-debug is set to yes.

host-port

Description The host-port subprofile specifies the physical address of the remote shelf. This profile is read-only.

Usage Following are the read-only fields in a profile for shelf 2:

```
[in REMOTE-SHELF-STAT/shelf-2:host-port]  
physical-address = { any-shelf any-slot 0 }  
logical-item = 0
```

I

id*

Description A subprofile that identifies the virtual channel link (VCL).

Usage Following is a listing of the `id` subprofile with its default settings:

```
[in ATM-VCL-CONFIG/{ { { any-shelf any-slot 0 } 0 } 0 0 }:id (new)]
address = { { any-shelf any-slot 0 } 0 }
vpi = 0
vci = 0
```

IDSL

Description A profile that enables you to configure ISDN digital subscriber line (IDSL) ports.

Usage Following is an example of the `idsl` profile with its default settings:

```
[in IDSL/{ shelf-1 slot-13 5 }]
name = 1:13:5
line-interface = { no [ {switched-channel 605 } { switched-channel 605 } ] +
physical-address* = { shelf-1 slot-13 5 }
sparing-mode = inactive
```

IDSL-STAT

Description A read-only profile that indicates the state of the ISDN digital subscriber line (IDSL) channels.

Usage Read-only. Following is a sample listing of an `idsl-stat` profile:

```
[in IDSL-STAT/{ shelf-1 slot-14 1 }]
physical-address* = { shelf-1 slot-14 1 }
line-state = point-to-point
channel-state = [ nailed-up nailed-up ]
error-count = [ 0 0 ]
spare-physical-address = { any-shelf any-slot 0 }
sparing-state = sparing-none
sparing-change-reason = unknown
sparing-change-time = 0
sparing-change-counter = 0
physical-status = { 444 }
physical-statistic = { { 0 0 6 } 107 [ 0 0 0 ] }
```

IF-SPARING-CONFIG

Description A profile that enables you to configure spare line interface modules (LIMs) using automatic sparing.

Usage Following is a listing of the if-sparing-config profile with its default settings:

```
[in IF-SPARING-CONFIG (new)]
if-spared-slot = [ any-slot any-slot any-slot any-slot any-slot any-sl+
if-spare-slot = [ any-slot any-slot any-slot any-slot any-slot any-slo+
if-auto-spare-info = [ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 +
lim-auto-spare-info = [ any-slot any-slot any-slot any-slot ot any-+
```

if-sparing-config

Description A read-only subprofile that contains the slot number of the redundant line interface module (LIM) for each LIM port.

Usage Following is a listing of an if-sparing-config subprofile:

```
[in LIM-SPARING-CONFIG/{ any-shelf any-slot 0 }:if-sparing-config (new)]
if-sparing-config[n] = any-slot
```

igmp-options

Description A subprofile that enables you to configure the timers defined in RFC 2236, *Internet Group Management Protocol Version 2*, on multicast client interfaces.

Usage Following is a listing of the igmp-options subprofile with its default settings:

```
[in CONNECTION/":ip-options:igmp-options]
robust-count = 2
query-interval = 125
query-response-interval = 100
last-member-query-interval = 10
last-member-query-count = 2
```

IMAGROUP

Description A profile that enables you to configure an inverse multiplexing over ATM (IMA) port. When you enter the command `new imagroup`, a new profile is created to establish all group-related IMA parameters.

Usage Following is a sample listing of an `imagroup` profile:

```
[in IMAGROUP/" (new)]
name* = ""
active = no
nailed-group = 0
group-symmetry-mode = symmetric-operation
version = vl-1
do-version-fallback = no
ignore-lineup = system-defined
lasr = yes
ne-tx-clk-mode = ctc
tx-min-num-links = 1
rx-min-num-links = 1
ima-id = 0
frame-length = 128
diff-delay-max = 25
check-far-end-ima-id = no
expected-far-end-ima-id = 0
far-end-check-frame-length = no
expected-far-end-frame-length = 128
atm-if-delay = 0
tpp-test-link = 0
tpp-test-pattern = -1
tpp-state = disabled
vp-switching-vpi = 15
```

IMA-GROUP-STAT

Description A profile that indicates the performance of an inverse multiplexing over ATM (IMA) group. The profile is automatically created by the system once the imagroup profile is properly configured and associated with a ds1-atm profile.

Usage Following is a sample listing of the ima-group-stat profile:

```
[in IMA-GROUP-STAT/ima3_1]
name* = ima3_1
physical-address = { shelf-1 slot-3 25 }
near-end-ima-group-state = operational
failure-status = no-failure
far-end-txclock-mode = ctc
tx-timing-ref-link = 0
rx-timing-ref-link = 0
rx-ima-id = 0
rx-frame-length = 128
least-delay-link = 0
diff-delay-max-obs = 0
running-secs = 1435
tx-avail-cellrate = 2147488176
rx-avail-cellrate = 4493
tx-num-config-links = 2
rx-num-config-links = 2
tx-num-active-links = 1
rx-num-active-links = 1
tx-oam-label-value = 3
rx-oam-label-value = 3
last-change-time = 52
tpp-test-link = 1
tpp-test-pattern = 100
tpp-test-status = link-fail
valid-intervals = 0
invalid-intervals = 96
vpi-vci-range = vpi-0-15-vci-32-127
vp-switching-vpi = 0
ima-group-statistic = { 40 0 6571424 }
nailed-group = 310
```

ima-group-statistic

Description A read-only subprofile that indicates the status of the inverse multiplexing over ATM (IMA) group.

Usage Read-only. Following is a sample listing of the ima-group-statistic subprofile:

```
[in IMA-GROUP-STAT:ima-group-statistic]
unavailable-secs = 56
near-end-num-failures = 3
far-end-num-failures = 6
```

IMAHW-CONFIG

Description A profile that enables you to configure hardware-specific parameters common to the inverse multiplexing over ATM (IMA) chip. For example, because the 24-port IMA line interface modules (LIMs) contain three chips, three profiles are created. However, the 8-port IMA LIMs contain a single chip so only one profile is created for it.

Usage Following is a listing of the imahw-config profile with sample settings:

```
[in IMAHW-CONFIG/{ any-shelf any-slot 0 } (new)]
name = ""
physical-address* = { any-shelf any-slot 0 }
alpha-ima-value = 2
beta-ima-value = 2
gamma-ima-value = 1
alpha-cell-delin-value = 7
delta-cell-delin-value = 6
```

ima-link-statistic

Description A read-only subprofile that indicates statistics for the inverse multiplexing over ATM (IMA) link.

Usage Read-only. Following is a sample listing of an imp-link-statistic subprofile:

```
[in DS1-ATM-STAT/{ shelf-1 slot-2 20 }:ima-link-statistic]
ima-violations-counter = 0
oif-anomalies-counter = 0
near-end-sev-errored-secs-counter = 0
far-end-sev-errored-secs-counter = 0
near-end-unavail-secs-counter = 0
far-end-unavail-secs-counter = 0
near-end-tx-unusable-secs-counter = 0
near-end-rx-unusable-secs-counter = 0
far-end-tx-unusable-secs-counter = 0
far-end-rx-unusable-secs-counter = 0
near-end-tx-num-failures-counter = 0
near-end-rx-num-failures-counter = 0
far-end-tx-num-failures-counter = 0
far-end-rx-num-failures-counter = 0
tx-stuffs-counter = 0
rx-stuffs-counter = 0
elapsed-seconds = 0
```


ima-link-status

Description A read-only subprofile that indicates the inverse multiplexing over ATM (IMA) link.

Usage Read-only. Following is a sample listing of an ima-link-status subprofile:

```
[in DS1-ATM-STAT/{ shelf-1 slot-2 20 }:ima-link-status]
near-end-tx-link-state = not-in-group
near-end-rx-link-state = not-in-group
far-end-tx-link-state = not-in-group
far-end-rx-link-state = not-in-group
near-end-rx-failure-status = no-failure
far-end-rx-failure-status = no-failure
tx-lid = 0
rx-lid = 0
relative-delay = 0
rx-test-pattern = 0
rx-testproc-status = disabled
valid-intervals = 96
invalid-intervals = 0
```

Location DS1-ATM-STAT

ima-option-config

Description A subprofile that enables you to configure an inverse multiplexing over ATM (IMA) interface.

Usage Following is a listing of an ima-option-config subprofile with sample settings:

```
[in DS1-ATM/{ any-shelf any-slot 0 }:line-config:ima-option-config (new)]
txlink-config = { 0 3 fast auto 10 0 }
rxlink-config = { 3 fast 10 100 auto 10 2500 10000 10 }
```

Location DS1-ATM/{ any-shelf any-slot 0 }:line-config

ima-rt

Description A read-only subprofile that indicates status of the inverse multiplexing over ATM (IMA) route.

Usage Following is a sample listing of the ima-rt subprofile:

```
[in IMA-GROUP-STAT:ima-rt]
name* = ima-rt
physical-address = { shelf-1 slot-2 25 }
near-end-ima-group-state = operational
far-end-ima-group-state = operational
failure-status = no-failure
far-end-txclock-mode = ctc
tx-timing-ref-link = 1
rx-timing-ref-link = 1
rx-ima-id = 0
rx-frame-length = 128
least-delay-link = 0
diff-delay-max-obs = 0
running-secs = 53461
tx-avail-cellrate = 7244
rx-avail-cellrate = 7188
tx-num-config-links = 2
rx-num-config-links = 2
tx-num-active-links = 2
rx-num-active-links = 2
tx-oam-label-value = 3
rx-oam-label-value = 3
last-change-time = 1315
tpp-test-link = 0
tpp-test-pattern = 255
tpp-test-status = disabled
valid-intervals = 0
invalid-intervals = 96
vpi-vci-range = vpi-0-15-vci-32-127
vp-switching-vpi = 15
ima-group-statistic = { 56 3 6 }
```

Location IMA-GROUP-STAT

immediate-mode-options

Description *Not used.*

Location TERMINAL-SERVER

index n

Description Index of the called device.

Usage Following is a listing of the `index` subprofile with its default settings:

```
[in CALL-ROUTE/{ { { shelf-1 any-slot 0 } 0 } 0 } :index]
device-address = { { shelf-1 any-slot 0 } 0 }
entry-number = 0
```

input-filters [n]

Description A subprofile that defines an input-filter specification. The filter specifications are applied in order (1 through 12) to the inbound packet stream. The order in which the input filters are defined is significant.

Usage To define an input filter specification, list the parameters of the subprofile as follows, and set the appropriate values:

```
[in FILTER/"" :input-filters[1]]
valid-entry = no
forward = no
Type = generic-filter
gen-filter = { 0 0 no no 00:00:00:00:00:00:00:00:00:00:00:00:00 00:00:00+
ip-filter = { 0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 none 0 none 0 no }
route-filter = { 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0 none }
tos-filter = { 0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 none 0 none 0 000 no+
ethernet-filter = { 00:00:00:00:00:00 00:00:00:00:00:00 00:00 }
```

integrity-config [n]

Description A subprofile for internal use only.

Location SYSTEM-INTEGRITY

interleave-path-config

Description A subprofile that enables you to configure minimum, maximum, and planned upstream and downstream bit rates for a rate-adaptive connection on an interleaved channel.

Usage Following is a listing of the `interleave-path-config` subprofile with its default settings:

```
[in AL-DMT/{ shelf-1 slot-4 1 } :interleave-path-config]
min-bitrate-up=0
min-bitrate-down=0
max-bitrate-up=0
max-bitrate-down=0
planned-bitrate-up=0
planned-bitrate-down=0
max-delay-up=16
max-delay-down=16
```

interval-performance-monitoring [n]

Description A read-only subprofile that indicates synchronous optical network (SONET) performance values for the preceding four 15-minute intervals, providing performance data for the past hour.

Usage Read-only. Following is a listing of the interval-performance-monitoring subprofile:

```
[in OC3-ATM-STAT/{ shelf-1 trunk-module-2 1 }:interval-performance-monitoring[1]]
sonet-section-errored-seconds=0
sonet-section-severely-errored-seconds=0
sonet-section-severely-errored-framing-seconds=0
sonet-section-coding-violations=0
sonet-line-errored-seconds=0
sonet-line-severely-errored-seconds=0
sonet-line-coding-violations=0
sonet-line-unavailable-seconds=0
sonet-far-end-line-errored-seconds=0
sonet-far-end-line-severely-errored-seconds=0
sonet-far-end-line-coding-violations=0
sonet-far-end-line-unavailable-seconds=0
sonet-path-errored-seconds=0
sonet-path-severely-errored-seconds=0
sonet-path-coding-violations=0
sonet-path-unavailable-seconds=0
sonet-far-end-path-errored-seconds=0
sonet-far-end-path-severely-errored-seconds=0
sonet-far-end-path-coding-violations=0
sonet-far-end-path-unavailable-seconds=0
```

Dependencies The information in the performance-monitoring subprofile updates the values in the interval-performance-monitoring subprofile.

ip-address-option

Description The ip-address-option subprofile contains a four-element array, with each element representing one pair of remote and local IP addresses.

Usage Following is a listing of the ip-address-option profile with its default settings:

```
[in CONNECTION/":bir-options:multiple-ip-address:ip-address-option (new)]
ip-address-option[1] = { 0.0.0.0/0 0.0.0.0/0 }
ip-address-option[2] = { 0.0.0.0/0 0.0.0.0/0 }
ip-address-option[3] = { 0.0.0.0/0 0.0.0.0/0 }
ip-address-option[4] = { 0.0.0.0/0 0.0.0.0/0 }
```

ip-address-option [n]

Description The ip-address-option[n] subprofile contains the destination IP address of a WAN virtual interface and the IP address of the local virtual interface.

Usage Following is a sample listing of an ip-address-option subprofile:

```
[in CONNECTION/":bir-options:multiple-ip-address:ip-address-option[1]
(new)]
remote-address = 0.0.0.0/0
netmask-remote = 0.0.0.0
local-address = 0.0.0.0/0
netmask-local = 0.0.0.0
```

ip-answer

Description A subprofile that enables you to configure the general settings to be used as defaults for incoming IP calls that do not specify a different value in the caller's profile

Usage Following is a listing of the ip-answer subprofile with its default settings:

```
[in ANSWER-DEFAULTS:ip-answer]
enabled = yes
vj-header-prediction = yes
assign-address = yes
routing-metric = 1
private-route-profile-required = no
```

ip-filter

Description An input-filter or output-filter subprofile for defining an IP packet filter.

Usage Set values in this subprofile to configure one of up to 12 input or output IP packet filters. Following is a listing of an ip-filter subprofile with its default settings:

- For input filters:

```
[in FILTER/":input-filters[1]:ip-filter]
protocol = 0
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
dest-address-mask = 0.0.0.0
dest-address = 0.0.0.0
Src-Port-Cmp = none
source-port = 0
Dst-Port-Cmp = none
dest-port = 0
tcp-estab = no
```

- For output filters:

```
[in FILTER/"":output-filters[1]:ip-filter]  
protocol = 0  
source-address-mask = 0.0.0.0  
source-address = 0.0.0.0  
dest-address-mask = 0.0.0.0  
dest-address = 0.0.0.0  
Src-Port-Cmp = none  
source-port = 0  
Dst-Port-Cmp = none  
dest-port = 0  
tcp-estab = no
```

IP-GLOBAL

Description A profile that enables you to configure the IP router systemwide.

Usage Following is a listing of the `ip-global` profile with its default settings:

```
[in IP-GLOBAL]
domain-name = ""
dns-primary-server = 0.0.0.0
dns-secondary-server = 0.0.0.0
dns-server-query-type = udp
system-ip-addr = 192.168.120.202
soft-ip-interface-addr = 0.0.0.0
netbios-primary-ns = 0.0.0.0
netbios-secondary-ns = 0.0.0.0
must-accept-address-assign = no
pool-summary = no
pool-chaining = no
pool-ospf-adv-type = type-1
pool-base-address = [ 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+
assign-count = [ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 +
pool-name = [ " " " " " " " " " " " " " " " " " " " " " " " "+
rip-policy = Poison-Rvrs
summarize-rip-routes = no
rip-trigger = yes
min-rip-trigger-delay = 5
max-rip-trigger-delay = 8
bootp-enabled = no
bootp-relay = { no [ 0.0.0.0 0.0.0.0 ] }
drop-source-routed-ip-packets = no
ignore-def-route = yes
rarp-enabled = no
udp-cksum = yes
tcp-timeout = 0
dialout-poison = no
telnet-password = ""
user-profile = admin
shared-prof = no
dns-list-attempt = no
```

```

static-pref = 100
rip-pref = 100
rip-queue-depth = 50
ospf-pref = 10
ospf-ase-pref = 150
ospf-global = { no yes 0 }
rip-tag = c8:00:00:00
rip-ase-type = 1
iproute-cache-enable = yes
iproute-cache-size = 0
ipport-cache-enable = yes
suppress-host-routes = no
snmp-info = { snmp-disabled utc+0000 [ 192.168.120.10 0.0.0.0 0.0.0.0 ] 10 }
dns-list-size = 6
client-primary-dns-server = 0.0.0.0
client-secondary-dns-server = 0.0.0.0
allow-as-client-dns-info = True
dns-local-table = { no no [ { "" 0.0.0.0 } { "" 0.0.0.0 } { "" 0.0.0.0 } { 0+
multicast-forwarding = no
mbone-profile = ""
mbone-lan-interface = { { any-shelf any-slot 0 } 0 }
multicast-hbeat-addr = 0.0.0.0
multicast-hbeat-port = 0
multicast-hbeat-slot-time = 0
multicast-hbeat-Number-Slot = 0
multicast-hbeat-Alarm-threshold = 0
multicast-hbeat-src-addr = 0.0.0.0
multicast-hbeat-src-addr-mask = 0.0.0.0
sec-domain-name = ""
multicast-member-timeout = 360
finger = no
ignore-icmp-redirects = no
icmp-reply-directed-bcast = yes
send-icmp-dest-unreachable = yes
global-vrouter = main
router-id = 0.0.0.0
default-filter-cache-time = 1440
default-prt-cache-time = 1440
tcp-syn-flood-protect = no
throttle-no-port-match-udp-traffic-on-slot = no
pim-options = { no no 0.0.0.0 0 60 }
multiple-mbone = { [ "" "" "" "" ] [ { { any-shelf any-slot 0 } 0 } { { +
multicast-forwarding = no
multiple-multicast-server-vc = no

```

IP-INTERFACE

Description A profile that enables you to configure a logical IP interface for an Ethernet port.

Usage Following is a listing of the ip-interface profile with its default settings:

```
[in IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }]  
interface-address* = { { any-shelf any-slot 0 } 0 }  
ip-address = 0.0.0.0/0  
proxy-mode = Off  
rip-mode = routing-off  
route-filter = ""  
rip2-use-multicast = yes  
multicast-allowed = no  
multicast-rate-limit = 100  
multicast-group-leave-delay = 0  
directed-broadcast-allowed = yes  
vrouter = ""  
management-only-interface = no  
qos-interface-group = 0  
packet-flows = ""
```

Dependencies Consider the following:

- For ip-interface profiles, the default profile (with the zero logical-item number) must have an IP address configured, or none of the other ip-interface profiles for the same port will function. Do not delete the default profile if you want your other configurations to work.
- If proxy-mode is enabled in any of the ip-interface profiles for a given Ethernet port, it is enabled for all ARP requests coming into the physical port.

ip-options

Description A subprofile that enables you to configure connection-specific IP-routing settings.

Usage Following is a listing of the `ip-options` subprofile with its default settings:

```
[in CONNECTION/"" :ip-options]
ip-routing-enabled = yes
vj-header-prediction = yes
remote-address = 0.0.0.0/0
local-address = 0.0.0.0/0
source-if = ""
routing-metric = 1
preference = 60
down-preference = 120
private-route = no
address-pool = 0
ip-direct = 0.0.0.0
rip = routing-off
route-filter = ""
source-ip-check = no
reverse-path-check = no
multicast-allowed = no
multicast-rate-limit = 100
multicast-group-leave-delay = 0
client-dns-primary-addr = 0.0.0.0
client-dns-secondary-addr = 0.0.0.0
client-dns-addr-assign = yes
client-default-gateway = 0.0.0.0
tos-options = { no 000 normal incoming precedence-tos 00 }
tos-filter = ""
client-wins-primary-addr = 0.0.0.0
client-wins-secondary-addr = 0.0.0.0
client-wins-addr-assign = yes
private-route-table = ""
private-route-profile-required = no
igmp-options = { 2 125 100 10 2 }
qos-interface-group = 0
packet-flows = ""
multicast-server-vc = no
multiple-mcast-filter = [ "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" ]
```

See Also `tos-options`

IP-ROUTE

Description A profile that defines a static IP route. The system adds the specified route to the routing table explicitly, rather than through dynamic updates when RIP is enabled on an interface. Static routes enable the system to communicate with another network without the added overhead of enabling RIP.

Usage Following is a listing of the ip-route profile with its default settings:

```
[in IP-ROUTE/" (new)]
name* = ""
dest-address = 0.0.0.0/0
netmask = 0.0.0.0
gateway-address = 0.0.0.0
metric = 8
cost = 1
preference = 60
third-party = no
ase-type = type-1
ase-tag = c0:00:00:00
private-route = no
active-route = yes
ase7-adv = N/A
vrouter = ""
inter-vrouter = ""
```

L

l2tp-config

Description An l2-tunnel-global subprofile for configuring Layer 2 Tunneling Protocol (L2TP) timers, retry parameters for tunnel establishment, and other L2TP access concentrator (LAC) operations. These settings affect the system in all L2TP negotiations. They are not specific to one L2TP network server (LNS).

Usage Following is a listing of the l2tp-config subprofile with its default settings:

```
[in L2-TUNNEL-GLOBAL:l2tp-config]
first-retry-timer = 1000
retry-count = 6
hello-timer = 60
control-connect-establish-timer = 60
lac-incoming-call-timer = 60
base-udp-port = 0
dialout-auth-lns = no
dialout-send-profile-name = no
verify-remote-host-name = no
acct-tunnel-connection-encoding = normal
tunnel-server-pre-sccrq-lookup = no
```

L2-TUNNEL-GLOBAL

Description A profile that enables you to configure Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) operations globally. The parameters in the l2-tunnel-global profile are used for all LAC operations, such as global tunnel authentication. They are not specific to one L2TP network server (LNS).

Usage Following is a listing of the l2-tunnel-global profile with its default settings:

```
[in L2-TUNNEL-GLOBAL]
l2tp-mode = disabled
l2tp-auth-enabled = no
l2tp-rx-window = 0
l2tp-system-name = ""
l2tp-config = { 1000 6 60 60 60 0 no no no normal no }
```

lan-router-interface-address

Description Index of the vlan-ethernet profile to be used as the “router” VLAN interface in terms of traffic handling for this bridge group. The specified VLAN interface is the default path for uplinks from users to the VLAN, and is used in port blocking to prevent other, unintended uses of the other interfaces that are part of the VLAN. This setting and the wan-router-interface-address setting are mutually exclusive.

Usage Following is a listing of the lan-router-interface-address profile shown with default settings:

```
[in BRIDGE-GROUP/0:lan-router-interface-address (new)]
physical-address = { any-shelf any-slot 0 }
logical-item = 0
```

Dependencies If IGMP snooping is enabled, this must be the Ethernet interface on which downstream multicast streams are received.

layer2-classifier

Description A flow-list subprofile for defining classification rules to identify a specific layer 2 traffic flow.

Usage Following is a listing of the layer2-classifier subprofile shown with default settings:

```
[in FLOW-SERVICES/":flow-list[1]:layer2-classifier (new)]
vlan-id = 0
ethernet-priority = 0
ethernet-type = 00:00
```

LIM-SPARING-CONFIG

Description A profile that enables you to configure line interface module (LIM) redundancy (sparing) and designate the primary and secondary LIM.

Usage Following is a listing of the `lim-sparing-config` profile with its default settings:

```
[in LIM-SPARING-CONFIG/{ any-shelf any-slot 0 } (new)]
physical-address* = { any-shelf any-slot 0 }
spare-slot-type = unknown
sparing-mode = inactive
spare-slot-number = slot-16
manually-spared-slot-number = any-slot
if-sparing-config = [ any-slot any-slot any-slot any-slot slot any+
auto-lim-sparing-config = { [ { yes 10 100 3 12 } { yes 10 100 3 12 } { 10 +
```

lim-sparing-config n

Description A subprofile that enables you to configure the redundancy of up to 16 line interface modules (LIMs).

Usage Following is a listing of the `lim-sparing-config n` subprofile with its default settings:

```
[in LIM-SPARING-CONFIG/{ any-shelf any-slot 0 }:auto-lim-sparing-config:
lim-sparing-config[1] }
active = yes
error-averaging-period = 10
error-threshold = 100
up-down-threshold = 3
modem-failure-threshold = 12
```

LIM-SPARING-STATUS

Description A read-only profile that indicates whether line interface module (LIM) sparing is enabled, as well as the slot numbers of the primary and secondary LIMs.

Usage Read-only. Following is a listing of the `lim-sparing-status` profile with its default settings:

```
[in LIM-SPARING-STATUS]
spare-slot-type = none
sparing-mode = inactive
spare-slot-number = any-slot
spared-slot-number = any-slot
sparing-change-reason = unknown
sparing-change-time = 0
sparing-change-counter = 0
lim-sparing-status = [ { yes yes sparing-none } { yes yes sparing-none } { +
```

lim-sparing-status [n]

Description One of 16 port subprofiles that indicate the redundancy status of a given line interface module (LIM).

Usage Read-only. Following is a listing of the lim-sparing-status subprofile with its default settings:

```
[in LIM-SPARING-STATUS:lim-sparing-status[1]]
active = yes
lim-status-ok = yes
sparing-state = sparing-none
```

line-config

Description A subprofile that has a differing function depending on the profile that includes it.

- In an al-dmt, ds1-atm, hds12, sds1, and shds1 profile, the line-config subprofile configures the corresponding line interface module (LIM).
- In an ds3-atm, e3-atm and oc3-atm profile the line-config subprofile configures the lines for the corresponding trunk module.
- In an atm-internal profile the line-config subprofile configures an internal line.

Usage Following are listings of the line-config subprofiles with their default values:

- [in AL-DMT/{ any-shelf any-slot 0 }:line-config (new)]


```
trunk-group = 0
nailed-group = 1
vp-switching-vpi = 15
activation = static
call-route-info = { any-shelf any-slot 0 }
rate-adapt-mode-up = automatic-at-startup
rate-adapt-mode-down = automatic-at-startup
rate-adapt-ratio-up = 100
rate-adapt-ratio-down = 100
max-aggr-power-level-up = 13
max-aggr-power-level-down = 20
max-power-spectral-density = 40
line-code = auto-select
line-latency-down = fast
line-latency-up = fast
trellis-encoding = yes
gain-default = 20-db
upstream-start-bin = 6
upstream-end-bin = 31
downstream-start-bin = 32
downstream-end-bin = 255
loop-back = none
bit-swapping = no
fbm-dbm-mode = fbm
alcatel-us-413-boost = unknown
```

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

- [in DS1-ATM/{ any-shelf any-slot 0 }:line-config (new)]
frame-type = esf
encoding = b8zs
nailed-group = 4294967246
loopback = no-loopback
clock-source = not-eligible
clock-priority = high-priority
FDL = none
send-code = no-code
front-end-type = short-haul
line-length = 1-133
line-build-out = 0-db
pcm-mode = clear-channel
coset-enabled = yes
scrambling-enabled = no
hec-correction-enabled = no
vp-switching-vpi = 15
vc-oamf4-support = [yesyesyesyesyesyesyesyesyesyesyesyesyesyes+
ima-option-config = { { 0 3 fast auto 10 0 } { 3 fast 10 100 auto 10 +
status-change-trap-enable = no

- [in DS3-ATM/{ any-shelf any-slot 0 }:line-config (new)]
trunk-group = 9
nailed-group = 1
activation = static
call-route-info = { any-shelf any-slot 0 }
loopback = no-loopback
high-tx-output = no
receive-equalization = no
framer-mode = C-BIT-PLCP
vpi-vci-range = vpi-0-255-vci-32-8191
vc-switching-vpi = [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+
clock-source = not-eligible
clock-priority = middle-priority
cell-payload-scramble = yes
status-change-trap-enable = no

- [in E3-ATM/{ any-shelf any-slot 0 }:line-config (new)]
trunk-group = 9
nailed-group = 1
call-route-info = { any-shelf any-slot 0 }
loopback = no-loopback
high-tx-output = no
framer-mode = g832-adm
vpi-vci-range = vpi-0-255-vci-32-8191
vc-switching-vpi = [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+
clock-source = not-eligible
clock-priority = middle-priority

- ```

cell-payload-scramble = yes
status-change-trap-enable = no

```
- [in HDSL2/{ any-shelf any-slot 0 }:line-config (new)]
 

```

trunk-group = 0
nailed-group = 1
vp-switching-vpi = 15
activation = static
call-route-info = { any-shelf any-slot 0 }
unit-type = coe
ntr-enabled = no
clock-source = not-eligible
clock-priority = middle-priority
loop-back = none
margin = 2db
snext-margin = disable
rate-mode = auto
min-rate = 72000
max-rate = 2312000
gshdsl-standard-network-type = north-american-annex-a
annexb-anfp-enabled = no
gshdsl-psd-type = symmetric
master-binding-port = no

```
  - [in OC3-ATM/{ any-shelf any-slot 0 }:line-config (new)]
 

```

trunk-group = 0
nailed-group = 1
call-route-info = { any-shelf any-slot 0 }
loopback = no-loopback
framer-mode = sonet
framer-rate = STS-3c
tx-scramble-disabled = no
tx-cell-payload-scramble-disabled = no
loop-timing = no
vpi-vci-range = vpi-0-255-vci-32-8191
vc-switching-vpi = [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+
clock-source = not-eligible
clock-priority = middle-priority

```
  - [in SDSL/{ any-shelf any-slot 0 }:line-config (new)]
 

```

trunk-group = 0
nailed-group = 1
vp-switching-vpi = 15
activation = static
call-route-info = { any-shelf any-slot 0 }
data-rate-mode = singlebaud
max-rate = 784000
auto-base-rate = 272000
unit-type = coe
line-mode = atm
loop-back = none

```

```
■ [in SHDSL/{ any-shelf any-slot 0 }:line-config (new)]
 trunk-group = 0
 nailed-group = 1
 vp-switching-vpi = 15
 activation = static
 call-route-info = { any-shelf any-slot 0 }
 unit-type = coe
 ntr-enabled = no
 clock-source = not-eligible
 clock-priority = middle-priority
 loop-back = none
 margin = 2db
 snext-margin = disable
 rate-mode = auto
 min-rate = 72000
 max-rate = 2312000
 gshdsl-standard-network-type = north-american-annex-a
 annexb-anfp-enabled = no
 gshdsl-psd-type = symmetric
 master-binding-port = no
```

**Dependencies** Settings in the atm-internal profile currently apply only to ISDN digital subscriber line (IDSL) or router modules.

## LINE-DIAG

**Description** A profile that enables you to configure line testing settings.

**Usage** Following is a listing of the line-diag profile with its default settings:

```
[in LINE-DIAG/{ shelf-1 slot-13 1 }]
physical-address* = { shelf-1 slot-13 1 }
bert-timer = 1-minute
bert-enable = no
idt-enable = no
idt-num-of-msg = 1000
```

## LINE-DIAG-STAT

**Description** A read-only profile that indicates the state of the line diagnostics set in the line-diag profile.

**Usage** Read-only. Following is a listing of the line-diag-stat profile with its default settings:

```
[in LINE-DIAG-STAT/{ shelf-1 slot-13 1 }]
physical-address* = { shelf-1 slot-13 1 }
bert-operation-state = stopped
idt-operation-state = stopped
bert-error-counter = 0
idt-send-count = 0
idt-recv-count = 0
idt-error-counter = 0
```



line-interface

**Description** A subprofile that enables you to configure an ISDN digital subscriber line (IDSL).

**Usage** Following is a listing of the `line-interface` subprofile with its default settings:

```
[in IDSL/{ any-shelf any-slot 0 }:line-interface (new)]
enabled = no
dual-link = no
channel-config = [{ switched-channel 1 } { switched-channel 1 }]
dial-plan = 0
answer-number-1 = ""
answer-number-2 = ""
idsl-bandwidth = idsl-128
ignore-lineup = system-defined
```

## LINE-TESTS

**Description** A profile that activates either the galvanic isolation and multiport tone tests. Each line interface module (LIM) has a line-tests profile

**Usage** Following is a listing of a line-tests profile with its default settings:

```
[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 +
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 +
specific-ports = no
test-type = gal-iso
test-terminal = external-tester-terminal
activate-test = no
```

## LOAD-SELECT

**Description** A profile that enables you to configure which module images to load to flash memory when the `load tar` command is issued.

**Usage** Following is a listing of a `load-select` profile with its default settings:

- For all Stinger models except the Stinger MRT:

```
[in LOAD-SELECT]
unknown-cards = auto
sdsl-atm = auto
al-dmtadsl-atm = auto
sdsl-atm-v2 = auto
dadsl-atm-24 = auto
glite-atm-48 = auto
hdsl2 = auto
annexb-dmtadsl = auto
t1000 = auto
ima = auto
stngr-32-idsl = auto
40-dmt-ads1 = auto
48-dmt-ads1 = auto
72-shdsl = auto
72-ct-dmt-ads1 = auto
72-gs-dmt-ads1 = auto
32-dmt-aslam = auto
vdsl = auto
```

- For the Stinger MRT:

```
[in LOAD-SELECT]
unknown-cards = auto
mrt-dmt = auto
```



**Note** An explicit load command for a particular module type overrides the settings in the Load-Select profile.

## LOG

**Description** A profile that enables you to configure systemwide event-logging settings. Systemwide event logging includes the Stinger log buffer accessed by the `log` command, and any `syslog` host designated by the `log` profile.

**Usage** Following is a listing of a `log` profile with its default settings:

```
[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 local+
history-size = 0
```

## loopback-config

**Description** A subprofile that enables you to configure loopback test parameters.

**Usage** Following is a listing of a `loopback-config` subprofile with its default settings:

```
[in ATM-OAM/{ { any-shelf any-slot 0 } 0 0 }:loopback-config (new)]
enabled = no
loopback-level = segment
loopback-cells-per-test = 1
error-threshold = 0
restart-after-trap = no
total-loopback-tests = 1
test-iteration-interval = 30
```

## M

### magic-keys

**Description** A subprofile for internal use only.

**Usage** Read-only. Following is a sample listing of the magic-keys subprofile:

```
[in ATMPVC-STAT/unit1:magic-keys]
magic-keys[1] = 0
magic-keys[2] = 201326688
```

**See Also** vcc-members, vcc-members N

### margin-config

**Description** A subprofile that enables you to configure noise-margin values for asymmetric digital subscriber line (ADSL) line interface modules (LIMs).

**Usage** Following is a sample listing of a margin-config subprofile:

```
[in AL-DMT/{ shelf-1 slot-4 1 }:margin-config]
target-noise-margin-up=6
target-noise-margin-down=6
min-noise-margin-up=0
min-noise-margin-down=0
max-add-noise-margin-up=31
max-add-noise-margin-down=31
ra-downshift-margin-up=0
ra-downshift-int-up=0
ra-downshift-margin-down=0
ra-downshift-int-down=0
ra-upshift-margin-up=0
ra-upshift-int-up=0
ra-upshift-margin-down=0
ra-upshift-int-down=0
```

### MCAST-SERVICE

**Description** A profile that enables you to define sets of multicast destination addresses that can be accessed by multicast clients.

**Usage** Set values in this profile to configure destination filters. Support is included for at least 1008 active mcast-service profiles. Following is a listing of the mcast-service profile with its default settings:

```
[in MCAST-SERVICE/" " (new)]
service-name* = ""
active = no
snmp-trap-enable = no
filter-type = none
filter-list = [{ no 0.0.0.0 } { no 0.0.0.0 } { no 0.0.0.0 } { no 0.0.0 n+
```

## menu-mode-options

**Description** *Not used.*

**Location** `TERMINAL-SERVER`

## metrics-index

**Description** *Not supported.* A subprofile that contains a complex index value into the set of parameters associated with the metrics-tag and metrics-direction parameters.

**Usage** Following is a listing of the metrics-index subprofile with its default settings:

```
[in PNNI-METRICS/{ 0 0 incoming 0 }:metrics-index (new)]
node-index = 1
metrics-tag = 0
metrics-direction = incoming
metrics-index = 0
```

## MODEM

**Description** *Not used.*

## modem-configuration

**Description** *Not used.*

**Location** `TERMINAL-SERVER`

## mp-answer

**Description** *Not supported.*

**Location** `ANSWER-DEFAULTS`

## mp-options

**Description** *Not supported.* A connection subprofile containing settings for incoming MultiLink Protocol (MP) session requests.

**Usage** Following is a listing of the mp-options subprofile with its default settings. These settings are not supported in Stinger units.

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

## mpp-answer

**Description** *Not supported.* An answer-defaults subprofile containing default settings for incoming MultiLink Protocol Plus™ (MPP or MP+) session requests.

**Location** ANSWER-DEFAULTS

## mpp-options

**Description** *Not supported.* An answer-defaults subprofile containing default settings for incoming MultiLink Protocol Plus™ (MPP or MP+) session requests.

**Location** CONNECTION/""

## MULTI-LINK-FR

**Description** A profile that enables you to configure a frame relay connection with multiple links.

**Usage** Following is a listing of the multi-link-fr profile with its default settings:

```
[in MULTI-LINK-FR/"" (new)]
mfr-bundle-name* = ""
active = no
mfr-bundle-type = mfr-dte
max-bundle-members = 1
min-bandwidth = 0
```

## multiple-ip-address

**Description** The multiple-ip-address subprofile contains the elements used to statically configure up to four WAN virtual interfaces across a BIR connection.

**Usage** Following is a listing of the multiple-ip-address profile with its default settings:

```
[in CONNECTION/"" :bir-options:multiple-ip-address (new)]
enable = no
ip-address-option = [{ 0.0.0.0/0 0.0.0.0/0 } { 0.0.0.0/0 0.0.0.0/0 } { 0.0+
```

## multiple-mbone

**Description** A subprofile to specify the parameters used to configure multiple multicast backbone (MBONE) router interfaces.

**Usage** Following is a listing of the multiple-mbone subprofile with its default settings:

```
[in IP-GLOBAL:multiple-mbone]
mbone-profile = ["" "" "" ""]
mbone-lan-interface = [{ { any-shelf any-slot 0 } 0 } { { any-shelf any-slo+
```

## multiple-mcast-filter

**Description** An array of 20 indexed parameters that allows multiple filters to be applied in sequence on the same connection.

**Usage** Following is a listing of the multiple-mcast-filter profile shown with default settings:

```
[in CONNECTION/vlan-pvc-1:ip-options:multiple-mcast-filter]
multiple-mcast-filter[1] = ""
multiple-mcast-filter[2] = ""
multiple-mcast-filter[3] = ""
multiple-mcast-filter[4] = ""
multiple-mcast-filter[5] = ""
multiple-mcast-filter[6] = ""
multiple-mcast-filter[7] = ""
multiple-mcast-filter[8] = ""
multiple-mcast-filter[9] = ""
multiple-mcast-filter[10] = ""
multiple-mcast-filter[11] = ""
multiple-mcast-filter[12] = ""
multiple-mcast-filter[13] = ""
multiple-mcast-filter[14] = ""
multiple-mcast-filter[15] = ""
multiple-mcast-filter[16] = ""
multiple-mcast-filter[17] = ""
multiple-mcast-filter[18] = ""
multiple-mcast-filter[19] = ""
multiple-mcast-filter[20] = ""
```

## N

### node-pgl

**Description** A subprofile that enables you to configure the node peer group leader (PGL) in the Private Network-to-Network Interface (PNNI).

**Usage** Following is a listing of the node-pgl profile with its default settings:

```
[in PNNI-NODE-CONFIG/1:node-pgl]
leadership-priority = 0
parent-node-index = 0
init-time = 15
override-delay = 30
reelect-time = 15
```

### node-scope-mapping

**Description** *Not currently used.* A subprofile for specifying scope mapping information for the node.

**Usage** Following is a listing of the node-scope-mapping subprofile with its default settings:

```
[in PNNI-NODE-CONFIG/1:node-scope-mapping]
local-net = 96
local-net-plus-1 = 96
local-net-plus-2 = 96
site-minus-1 = 80
intra-site = 80
site-plus-1 = 72
organization-minus-1 = 72
intra-organization = 64
organization-plus-1 = 64
community-minus-1 = 64
intra-community = 48
community-plus-1 = 48
regional = 32
inter-regional = 32
global = 0
```



## node-svcc-rcc

**Description** *Not currently used.* A subprofile that specifies SVCC-based routing control channel (RCC) variables

**Usage** Following is a listing of the node-svcc-rcc subprofile with its default settings:

```
[in PNNI-NODE-CONFIG/1:node-svcc-rcc]
init-time = 4
retry-time = 30
calling-integrity-time = 5
called-integrity-time = 50traffic-descr-index = 0v
traffic-descr-index = 0
```

## node-timer

**Description** A subprofile that enables you to configure initial Private Network-to-Network Interface (PNNI) timer settings and significant change thresholds for the node.

**Usage** Following is a listing of the node-time subprofile with its default settings:

```
[in PNNI-NODE-CONFIG/1:node-timer]
ptse-holddown = 10
hello-holddown = 10
hello-interval = 15
hello-inactivity-factor = 5
hlink-inact = 120
ptse-refresh-interval = 1800
ptse-lifetime-factor = 200
rxmt-interval = 5
peer-delayed-ack-interval = 10
avcr-pm = 50
avcr-mt = 3
cdv-pm = 25ctd-pm = 50
ctd-pm = 50
```

**Location** PNNI-NODE-CONFIG N

# O

## OC3-ATM

**Description** A profile that enables you to configure settings for the OC3-ATM interface.

**Usage** Following is a listing of the oc3-atm profile with its default settings:

```
[in OC3-ATM/{ shelf-1 trunk-module-1 1 }]
name = 1:17:1
physical-address* = { shelf-1 trunk-module-1 1 }
enabled = no
spare-physical-address = { any-shelf any-slot 0 }
sparing-mode = inactive
ignore-lineup = system-defined
aps-config-name = pgl
```

## OC3-ATM-STAT

**Description** A read-only profile that indicates ATM framer status and error counters for an OC3-ATM interface.

**Usage** Read-only. Following is a sample listing of an oc3-atm-stat profile:

```
[in OC3-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 = unknown
sparing-change-time = 0
sparing-change-counter = 0
vpi-vci-range = vpi-0-255-vci-32-1023
vc-switching-vpi = "0 10 20 30 40 50"
vcc-vpi = [0 0 0 0 0 0 0 0 0 0 0 10 0 0 0 0 0 0 0 0 0 20 0 0 0 0 0 0 0 0 0 30+
aps-config-name = ""
aps-channel-status = unknown
aps-channel-sd-condition = False
aps-channel-sf-condition = False
aps-channel-low-direction = low-none
aps-channel-recv-sd-count = 0
aps-channel-recv-sf-count = 0
aps-channel-recv-ais-count = 0
aps-channel-recv-rdi-count = 0
loss-of-signal = False
loss-of-frame = False
out-of-frame = False
section-state = sonet-section-active-no-defect
path-state = sonet-path-active-no-defect
ais-receive = False
yellow-receive = False
out-of-cell-delineation = False
```

```

loss-of-cell-delineation = False
aps-receive = False
rsop-bip-error-count = 0
rlop-bip-error-count = 0
rlop-febe-error-count = 0
rpop-bip-error-count = 0
rpop-febe-error-count = 0
racp-chcs-error-count = 0
racp-uchcs-error-count = 0
racp-rx-cell-count = 0
tacp-tx-cell-count = 0
frequency-justification-count = 3
HEC-cell-drop-counter = 0
FIFO-overflow-counter = 0
idle-cell-counter = 3778231663
valid-cell-counter = 280935
time-elapsed = 191
performance-monitoring = { 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 }
interval-performance-monitoring = [{ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 }

```

## ospf

**Description** A subprofile that enables you to configure Open Shortest Path First (OSPF) routing on an Ethernet interface.

**Usage** Following is a listing of an ospf subprofile with its default settings:

```

[in IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf (new)]
active = no
area = 0.0.0.0
area-type = normal
hello-interval = 10
dead-interval = 40
priority = 5
authen-type = simple
auth-key = ascend0
key-id = 0
cost = 1
down-cost = 16777215
ase-type = type-1
ase-tag = c0:00:00:00
transit-delay = 1
retransmit-interval = 5
non-multicast = no
network-type = Broadcast
poll-interval = 10
profile-type = lan
md5-auth-key = ascend0

```

## OSPF-AREA-RANGE

**Description** A profile that enables you to define an area within an Open Shortest Path First (OSPF) autonomous system.

**Usage** Following is a listing of an ospf-area-range profile with its default settings:

```
[in ospf-area-range/" (new)]
name* = ""
area-id = 0.0.0.0
area-network-addr = 0.0.0.0/0
area-network-mask = 0.0.0.0
advertize = no
```

## ospf-global

**Description** A subprofile that enables you to define global Open Shortest Path First (OSPF) behavior.

**Usage** Following is a listing of an ospf-global subprofile with its default settings:

```
[in IP-GLOBAL:ospf-global (new)]
enable = no
as-boundary-router = yes
ospf-set-trap = 00:00:00:00
ospf-max-lsa = 0
```

## OSPF-NBMA-NEIGHBOR

**Description** A profile that enables you to configure an Open Shortest Path First (OSPF) router for operation on a nonbroadcast multiaccess (NBMA) network.

**Usage** Following is a listing of an ospf-nbma-neighbor profile with its default settings:

```
[in ospf-nbma-neighbor/" (new)]
name* = ""
host-name = ""
ip-address = 0.0.0.0
dr-capable = no
```

## ospf-options

**Description** A subprofile that contains settings for Open Shortest Path First (OSPF) routing.

**Usage** Following is a listing of an ospf-options subprofile with its default settings:

```
[in CONNECTION/":ip-options:ospf-options (new)]
active = no
area = 0.0.0.0
area-type = normal
hello-interval = 30
dead-interval = 120
priority = 5
authen-type = simple
auth-key = ascend0
key-id = 0
cost = 10
down-cost = 1000
ase-type = type-1
ase-tag = c0:00:00:00
transit-delay = 1
retransmit-interval = 5
non-multicast = no
network-type = Point-to-Point
poll-interval = 10
md5-auth-key = ascend0
```

## OSPF-VIRTUAL-LINK

**Description** A profile that includes settings for creating Open Shortest Path First (OSPF) virtual connections .

**Usage** Following is a listing of an ospf-virtual-link profile with its default settings:

```
[in OSPF-VIRTUAL-LINK/0.0.0.0 (new)]
neighbor-router-id* = 0.0.0.0
transit-area-id = 0.0.0.0
rexmit-delay = 5
xmit-delay = 1
hello-interval = 30
dead-interval = 120
authen-type = simple
authen-key = ascend0
key-id = 0
md5-authen-key = ascend0
```

## outgoing-queue [n]

**Description** A subprofile that enables you to configure Asynchronous Transfer Mode (ATM) for an outgoing queue. Each configured queue must be associated with an outgoing port that is either a control module slot or a trunk port. Each outgoing port can have multiple outgoing queues.

**Usage** Following is a listing of the outgoing-queue subprofile with its default settings:

```
[in SWITCH-CONFIG/tram-18:atm-parameters:outgoing-queue[1]]
active = yes
name = 1:18:1
physical-address = { shelf-1 trunk-module-2 1 }
cbr = yes
real-time-vbr = no
non-real-time-vbr = no
ubr = no
high-priority-weight = 5
low-priority-weight = 0
source-port = { shelf-1 trunk-module-2 2 }
hop-level = any-level
```

## outgoing-shaper [n]

**Description** A subprofile that enables you to configure the shapers available for the entire system. A trunk port might use zero, one, or more shaper(s) to shape outgoing Asynchronous Transfer Mode (ATM) traffic with certain virtual path identifiers (VPIs).

**Usage** Following is a listing of the outgoing-shaper subprofile with its default settings:

```
[in SWITCH-CONFIG:atm-parameters:outgoing-shaper[1] (new)]
queue-index = 0
vpi = 1
bandwidth = 8000
```

## output-filters [n]

**Description** A subprofile that defines an output-filter specification. The filter specifications are applied in order (1 through 12) to the inbound packet stream. The order in which the output filters are defined is significant.

**Usage** To define an output filter specification, list the parameters of the subprofile as follows, and set the appropriate values:

```
[in FILTER/"":output-filters[1]]
valid-entry = no
forward = no
Type = generic-filter
gen-filter = { 0 0 no no 00:00:00:00:00:00:00:00:00:00:00:00:00:00 00:00:00+
ip-filter = { 0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 none 0 none 0 no }
route-filter = { 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0 none }
tos-filter = { 0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 none 0 none 0 000 no+
ethernet-filter = { 00:00:00:00:00:00 00:00:00:00:00:00 00:00 }
```

## P

### packet-classifier

**Description** Specifies a classification rule.

**Usage** Following is a listing of the packet-classifier profile shown with default settings:

```
[in PACKET-FLOWS/"":flow[1]:packet-classifier (new)]
interface-group = 0
source-ip-address = 0.0.0.0/0
source-ip-netmask = 0.0.0.0
destination-ip-address = 0.0.0.0/0
destination-ip-netmask = 0.0.0.0
ip-protocol = 0
ip-tos = 0
source-port-comparison = none
source-port = 0
destination-port-comparison = none
destination-port = 0
```

### packet-flows

**Description** The packet-flows profile defines classifications by input interface, packet content, or both, and assigns corresponding scheduling priorities.

**Usage** Following is a listing of the packet-flows profile shown with default settings:

```
[in PACKET-FLOWS/" " (new)]
name* = ""
marking-type = none
flow = [{ { 0 0 00:00 } { 0 0.0.0.0/0 0.0.0.0/0 0 0 none 0 none 0 } { 0 } } +
global-packet-marking = [{ 0 0 0 } { 1 0 0 } { 2 0 0 } { 3 0 0 } { 4 0 0 } {+
exception-packet-marking = { 8 0 0 }
```

### password-profile

**Description** A subprofile of external-auth containing settings for calling line ID (CLID) and Dialed Number Information Service (DNIS) passwords set in a RADIUS profile.

**Usage** Following is a listing of a password-profile subprofile with its default settings:

```
[in EXTERNAL-AUTH:password-profile]
clid = ""
dnis = ""
banner = *****
init-banner = *****
pool = *****
frdl = *****
dialout = *****
dialout-routes = *****
```



## performance-monitoring

**Description** A read-only subprofile that indicates cumulative synchronous optical network (SONET) performance counters, which are reset at the end of every 15-minute interval.

**Usage** Read-only. Following is a listing of the performance-monitoring subprofile with its default settings:

```
[in OC3-ATM-STAT/{ shelf-1 trunk-module-2 1 }:performance-monitoring]
sonet-section-errored-seconds=0
sonet-section-severely-errored-seconds=0
sonet-section-severely-errored-framing-seconds=0
sonet-section-coding-violations=0
sonet-line-errored-seconds=0
sonet-line-severely-errored-seconds=0
sonet-line-coding-violations=0
sonet-line-unavailable-seconds=0
sonet-far-end-line-errored-seconds=0
sonet-far-end-line-severely-errored-seconds=0
sonet-far-end-line-coding-violations=0
sonet-far-end-line-unavailable-seconds=0
sonet-path-errored-seconds=0
sonet-path-severely-errored-seconds=0
sonet-path-coding-violations=0
sonet-path-unavailable-seconds=0
sonet-far-end-path-errored-seconds=0
sonet-far-end-path-severely-errored-seconds=0
sonet-far-end-path-coding-violations=0
sonet-far-end-path-unavailable-seconds=0
```

## permit-list

**Description** Configure up to 20 entries in the tac1 profile, each of which specifies a source IP address that is explicitly allowed telnet access to the system.

**Usage** Following is a listing of the permit-list profile shown with default settings:

```
[in TACL:permit-list (new)]
permit-list[1] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[2] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[3] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[4] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[5] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[6] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[7] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[8] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[9] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[10] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[11] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[12] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[13] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[14] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[15] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[16] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[17] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[18] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[19] = { no 0.0.0.0/0 0.0.0.0 }
permit-list[20] = { no 0.0.0.0/0 0.0.0.0 }
```

## permit-list [n]

**Description** Specify a source IP address that is explicitly allowed telnet access to the system.

### Usage

```
[in TACL:permit-list [n] (new)]
valid-entry = no
source-address = 0.0.0.0/0
source-address-mask = 0.0.0.0
```

## physical-statistic

**Description** A read-only subprofile of the al-dmt-stat, hds12-stat, and sds1-stat profiles that reports statistics about xDSL performance.

**Usage** A read-only profile. Following is a sample listing of the each of the different physical-statistics subprofiles for the asymmetric digital subscriber line (ADSL), HDSL2, and SDSL line interface modules (LIMs):

- [in AL-DMT-STAT/{ shelf-1 slot-11 21 }:physical-statistic]  
line-up-timer = { 0 1 4 }  
rx-signal-present = yes  
up-dwn-cntr = 1  
self-test = passed  
noise-margin-down = 112  
attenuation-down = 1  
output-power-down = 7  
noise-margin-up = 9  
attenuation-up = 1  
output-power-up = 11  
near-end-fec = 0  
near-end-crc = 1  
near-end-hec = 0  
far-end-fec = 0  
far-end-crc = 0  
far-end-hec = 0  
received-rs-blocks = 15887016  
transmitted-rs-blocks = 15887016  
incoming-cells = 5097739  
outgoing-cells = 13989942
- [in HDSL2-STAT/{ shelf-1 slot-3 21 }:physical-statistic]  
line-up-timer = { 0 1 11 }  
rx-signal-present = yes  
line-quality = 41  
up-dwn-cntr = 1  
self-test = passed  
transmit-power = 10  
framer-sync-status = in-sync  
code-violations = 0  
errored-second = 0  
severely-errored-second = 0  
losw-second = 1  
unavailable-second = 0  
loop-attenuation = 107  
snr-margin = 42  
stur-loop-attenuation = 0  
stur-snr = 40
- [in IDSL-STAT/{ shelf-1 slot-14 1 }:physical-statistic]  
line-up-timer = { 0 0 6 }  
up-dwn-cntr = 107  
error-count = [ 0 0 0 ]

- [in SDSL-STAT { shelf-1 slot-1 0 }:physical-statistic]  
line-up-timer={ 1 13 55 }  
rx-signal-present=yes  
line-quality=15  
up-dwn-cntr=0  
self-test=passed  
far-end-db-attenuation=4  
firmware-startup-stage=normal-operation  
bert-timer=2 minutes  
bert-enable=no  
bert-operation-state=stopped  
bert-error-counter=0
- [in SHDSL-STAT/{ shelf-1 slot-3 21 }:physical-statistic]  
line-up-timer = { 0 1 11 }  
rx-signal-present = yes  
line-quality = 41  
up-dwn-cntr = 1  
self-test = passed  
transmit-power = 10  
framer-sync-status = in-sync  
code-violations = 0  
errored-second = 0  
severely-errored-second = 0  
losw-second = 1  
unavailable-second = 0  
loop-attenuation = 107  
snr-margin = 42  
stur-loop-attenuation = 0  
stur-snr = 40

**See Also** `physical-status`

## physical-status

**Description** A read-only subprofile of the al-dmt-stat, hdsl2-stat, and sdsl-stat profiles that reports the status of XDSL interfaces.

**Usage** A read-only profile. Following is a sample listing of the each of the different physical-status subprofiles for the asymmetric digital subscriber line (ADSL), HDSL2, and SDSL line interface modules (LIMs):

- [in AL-DMT-STAT/{ shelf-1 slot-11 21 }:physical-status]  
 if-group-index = 367  
 unit-type = coe  
 dev-line-state = port-up  
 up-stream-rate-fast = 800000  
 down-stream-rate-fast = 7744000  
 up-stream-rate-interleaved = 0  
 down-stream-rate-interleaved = 0  
 up-stream-latency = fast  
 down-stream-latency = fast  
 firmware-ver = 069.5  
 ansi-adsl-ver = 2  
 initial-adsl-ver = 1  
 hardware-ver = 5  
 modem-hw-state = init-ok  
 accum-bit-err = 0  
 num-sec-valid = 3886  
 num-sec-invalid = 0  
 operational-mode = ansi-alcatel-1-4-1  
 last-state-change = { { 15 34 42 } { Wednesday April 2004 14 } }
- [in HDSL2-STAT/{ shelf-1 slot-3 21 }:physical-status]  
 if-group-index = 143  
 unit-type = coe  
 interface-type = hdsl2  
 dev-line-state = port-up  
 operational-rate = 1544000  
 firmware-ver = "B64 "  
 hardware-ver = 0  
 network-type = annex-b-anfp  
 last-state-change = { { 15 34 42 } { Wednesday April 2004 14 } }
- [in IDSL-STAT/{ shelf-1 slot-14 1 }:physical-status]  
 if-group-index = 444  
 last-state-change = { { 15 34 42 } { Wednesday April 2004 14 } }
- [in SDSL-STAT { shelf-1 slot-1 0 }:physical-status ]  
 if-group-index=0  
 unit-type=coe  
 dev-line-state=port-up  
 up-stream-rate=784000  
 down-stream-rate=784000  
 major-firmware-ver=13  
 minor-firmware-ver=2  
 hardware-ver=2  
 last-state-change = { { 15 34 42 } { Wednesday April 2004 14 } }

```
■ [in SHDSL-STAT/{ shelf-1 slot-2 10 }:physical-status]
 if-group-index = 226
 unit-type = coe
 interface-type = g-shdsl
 dev-line-state = startup-handshake
 operational-rate = 0
 firmware-ver = "R2.0 "
 hardware-ver = 0
 network-type = annex-a
 last-state-change = { { 15 34 42 } { Wednesday April 2004 14 } }
```

**See Also** `physical-statistic`

## `pim-group-rp-mapping`

**Description** A profile to configure associations between groups and rendezvous points (RPs). These static mappings provide a basic interoperability mechanism if the automatic methods of obtaining mappings should fail.

Each `pim-group-rp-mapping` profile specifies a mapping between an RP (specified as a reachable IP address) and a range of multicast groups (specified as a group and mask). The system uses these mappings to determine an RP for a given group.

**Usage** Following are the parameters, shown with their default settings, for configuring a static group-to-RP mapping:

```
[in PIM-GROUP-RP-MAPPING/""]
name* = ""
rp-address = 0.0.0.0
group-address = 0.0.0.0/0
group-mask = 0.0.0.0
```

## `pim-options`

**Description** Subprofiles for enabling Protocol Independent Multicast sparse mode (PIM-SM) on a Stinger unit.

**Usage** Following are sample listings of `pim-options` profiles:

```
[in IP-GLOBAL:pim-options]
enable = no
cbsr-enable = no
cbsr-ip-address = 0.0.0.0
cbsr-priority = 0
cbsr-interval = 60

[in IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:pim-options]
enable = no
hello-interval = 30
hello-hold-time = 105
hello-priority-option = yes
hello-priority = 1
join-prune-interval = 60
join-prune-hold-time = 210
```

```
lan-delay-option = yes
lan-delay = 5000
override-interval = 2500
```

## PNNI-IF-CONFIG

**Description** A profile that enables you to configure a Private Network-to-Network Interface (PNNI).

**Usage** Following is a sample listing of the `pnni-if-config` profile:

```
[in PNNI-IF-CONFIG/{ { any-shelf any-slot 0 } 0 } (new)]
address* = { { any-shelf any-slot 0 } 0 }
if-node-index = 1
if-aggr-token = 0
if-vp-capability = true
if-adm-weight-cbr = 5040
if-adm-weight-rt-vbr = 5040
if-adm-weight-nrt-vbr = 5040
if-adm-weight-abr = 5040
if-adm-weight-ubr = 5040
if-rcc-service-category = nrt-vbr
if-rcc-qos-name = default-ctl
external-change = no
```

## PNNI-METRICS

**Description** A profile that enables you to configure the attachment of settings for routing metrics and attributes for Private Network-to-Network Interface (PNNI) nodes, links, and reachable addresses.

**Usage** Following is a sample listing of a `pnni-metrics` profile:

```
[in PNNI-METRICS/{ 1 0 incoming 0 }]
metrics-index* = { 1 0 incoming 0 }
metrics-classes = 0
metrics-gcac-clp = clpequal0or1
metrics-admin-weight = 5040
metrics1 = 4294967295
metrics2 = 4294967295
metrics3 = 4294967295
metrics4 = 4294967295
metrics5 = 4294967295
metrics6 = 4294967295
metrics7 = 4294967295
metrics8 = 4294967295
external-change = no
active = no
```

## PNNI-NODE-CONFIG

**Description** A profile that enables you to configure settings that affect Private Network-to-Network Interface (PNNI) node operations.

**Usage** Following is a listing of the pnni-node-config profile with its default settings:

```
[in PNNI-NODE-CONFIG/1]
node-index* = 1
node-level = 96
node-id = 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00+
curr-node-id =
48:a0:39:84:0f:80:01:bc:72:00:01:d0:6a:96:00:ff:d0:6a:+
node-lowest = true
node-admin-status = up
node-domain-name = ""
node-atm-address =
39:84:0f:80:01:bc:72:00:01:d0:6a:96:00:ff:d0:6a:96+
node-peer-group-id = 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
curr-node-peer-group-id = 48:39:84:0f:80:01:bc:72:00:01:00:00:00:00:00
node-restricted-transit = false
node-complex-rep = false
node-pgl = { 0 0 15 30 15 }
node-timer = { 10 10 15 5 120 1800 200 5 10 50 3 25 50 }
node-svcc-rcc = { 4 30 35 50 0 }
node-scope-mapping = { 96 96 35 80 80 72 72 64 64 64 48 48 32 0 0 }
```

**See Also** node-pgl, node-scope-mapping, node-svcc-rcc, node-timer

## pnni-node-prefix

**Description** A subprofile that contains the system or manually generated value used as the prefix for the default node Asynchronous Transfer Mode (ATM) address.

**Usage** Following is a listing of a pnni-node-prefix subprofile with its default settings:

```
[in ATM-PREFIX/default:pnni-node-prefix]
length = 13
address = 39:84:0f:80:01:bc:72:00:01:00:00:00:00:00
```

**See Also** spvc-addr-prefix, svc-addr-prefix



## PNNI-ROUTE-ADDR

**Description** A profile that enables you to configure Private Network-to-Network Interface (PNNI) reachable addresses. A *reachable address* is an Asynchronous Transfer Mode (ATM) address that can be reached either directly through one of the unit's interfaces or through an advertising node that the unit can reach. You can configure a static route to a reachable address prefix, which enables the unit to reach all ATM addresses for end systems and other nodes whose ATM addresses match the prefix.

**Usage** Following is a listing of the `pnni-route-addr` profile with its default settings:

```
[in PNNI-ROUTE-ADDR/" (new)]
name* = ""
addr-index = { 0 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0+
if-index = 0
adv-node-id= 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
adv-port-id = 0
type = exterior
proto = other
pnni-scope = 0
vp-capability = false
metrics-tag = 0
ptse-id-ptse-id = 0
originate-advert = true
info = ""
oper-status = inactive
time-stamp = 0
external-change = no
active = no
```

**See Also** `addr-index`

## PNNI-ROUTE-TNS

**Description** A profile that enables you to configure a static route to a Private Network-to-Network Interface (PNNI) transit network. A *transit network* lies between the networks of the two end points of a connection. A connection's data transits the network, but does not originate or stop there.

**Usage** Following is a listing of the `pnni-route-tns` profile which includes a listing of its associated subprofile.

```
[in PNNI-ROUTE-TNS/{ 0 other other 00:00:00:00 0 }]
tns-index* = { 0 other other 00:00:00:00 0 }
tns-if-index = 0
tns-advertising-node-id = 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:
tns-advertised-port-id = 0
tns-route-type = exterior
tns-pnni-scope = 0
tns-vp-capability = no
tns-metrics-tag = 0
tns-originate-advertisement = yes
active = no
```

## PNNI-SUMMARY-ADDR

**Description** A profile that explicitly configures summary addresses.

**Usage** Following is a listing of the pnni-summary-addr profile with its default settings:

```
[in PNNI-SUMMARY-ADDR/""]
index-name* = ""
addr-index = { 1 internal-summary 00:00:00:00:00:00:00:00:00:00:00:00+
suppress = false
state = inactive
active = no
```

**See Also** addr-index

## port-redirect-options

**Description** A subprofile that enables you to redirect certain packet types to a specified server. For example, you can redirect Hypertext Transfer Protocol (HTTP) traffic to a Web cache server on a local network. You can use the port redirection capability to redirect any TCP or UDP packet on the basis of its protocol and port information.

**Usage** Following is a listing of the port-redirect-options subprofile with its default settings:

```
[in CONNECTION/"":port-redirect-options]
protocol = none
port-number = 0
redirect-address = 0.0.0.0
```

## ppp-answer

**Description** A subprofile that enables you to configure default settings for incoming PPP session requests. You set values in this subprofile to specify general values to be used as defaults for incoming PPP session requests that do not specify a different value in the caller's profile.

**Usage** Following is a listing of the ppp-answer subprofile with its default settings:

```
[in ANSWER-DEFAULTS:ppp-answer]
enabled = yes
receive-auth-mode = no-ppp-auth
bi-directional-auth = none
substitute-send-name = ""
disconnect-on-auth-timeout = yes
bridging-group = 0
link-compression = none
mru = 1524
lqm = no
lqm-minimum-period = 600
lqm-maximum-period = 600
mtu = 1524
max-pap-auth-retry = 0
```

## pppoe-options

**Description** A subprofile of the connection and the ethernet profiles that enables a router module to process PPP over Ethernet (PPPoE) packets, as defined in RFC 2516

**Usage** Following are listings of both versions of the subprofile:

- Following is a listing of the CONNECTION/"" :pppoe-options subprofile with its default settings:

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

- Following is a listing of the ETHERNET/{ any-shelf any-slot 0 } :pppoe-options subprofile with its default settings:

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

## pppoe-snooping

**Description** The pppoe-snooping subprofile configures the system to snoop incoming PPPoE Discover packets (Ether Type 0x8863) on connections and adds vendor-specific information before bridging packets to an upstream interface.

**Usage** Following is a listing of the pppoe-snooping profile with its default settings:

```
[in BRIDGE-GROUP/0 :pppoe-snooping (new)]
enable = no
circuit-id = { no 0.0.0.0 "" 1 no }
remote-id = { no 0.0.0.0 "" 1 no }
```

## ppp-options

**Description** A subprofile that enables you to configure the Stinger unit to establish a connection that uses Point-to-Point Protocol (PPP) authentication.

**Usage** Following is a listing of the ppp-options subprofile with its default settings:

```
[in CONNECTION/":ppp-options]
send-auth-mode = no-ppp-auth
ppp-circuit = none
ppp-circuit-name = ""
bi-directional-auth = none
send-password = ""
substitute-send-name = ""
recv-password = ""
substitute-recv-name = ""
link-compression = stac
mru = 1524
lqm = no
lqm-minimum-period = 600
lqm-maximum-period = 600
split-code-dot-user-enabled = no
mtu = 1524
```

## preferred-source

**Description** A subprofile that enables you to configure the address of a device within the system. Calls that originate at the preferred source may be routed to the indexed destination.

**Usage** Following is a listing of the preferred-source subprofile with its default settings:

```
[in CALL-ROUTE/{ { { shelf-1 any-slot 0 } 0 } 0 }:preferred-source]
physical-address = { any-shelf any-slot 0 }
logical-item = 0
```

## PRIVATE-ROUTE-TABLE

**Description** A profile that enables you to configure a private routing table. Specific connection or radius profiles can refer to a private routing table by name to have access to its routes.

**Usage** Following is a listing of the private-route-table profile with its default setting:

```
[in PRIVATE-ROUTE-TABLE/"]
name* = ""
route-description-list = [{ no 0.0.0.0/0 0.0.0.0 0.0.0.0 0 } { no 0.+
```

## psd-frequency-level

**Description** A subprofile of the `clt-result` profile that contains the results of the PSD test for the copper loop test (CLT) module.

**Usage** Following is a sample listing of the subprofile:

```
[in CLT-RESULT:psd-frequency-level [1] (new)]
frequency = 0
level = 0
```

## Q

### q2931-options

**Description** A subprofile of atm-if-sig-params containing Q.2931 parameters specifying the timers and retry values associated with the functionality of the Q.2931 signaling layer.

**Usage** Following is a listing of a q2931-options subprofile with its default settings:

```
[in ATM-IF-SIG-PARAMS/{ { any-shelf any-slot 0 } 0 }:q2931-options (new)]
ax-restart = 2
ax-statenq = 1
301-ms = 180000
303-ms = 4000
306-ms = 30000
308-ms = 30000
309-ms = 10000
310-ms = 10000
313-ms = 30000
316-ms = 120000
317-ms = 60000
322-ms = 4000
331-ms = 60000
333-ms = 10000
397-ms = 180000
398-ms = 4000
399-ms = 14000
aal-retry-ms = 10000
303-num-retries = 1
308-num-retries = 1
316-num-retries = 1
```

## qsaal-options

**Description** A subprofile of atm-if-sig-parms that contains the Q.SAAL parameters that specify the timers and retry values associated with the functionality of the Q.SAAL layer.

**Usage** Following is a listing of the qsaal-options subprofile with its default values:

```
[in ATM-IF-SIG-PARAMS/{ { any-shelf any-slot 0 } 0 }:qsaal-options (new)]
window-size = 50
max-cc = 4
max-pd = 25
max-stat = 67
tcc-ms = 1000
tpoll-ms = 0
tkeepalive-ms = 0
tnoresponse-ms = 0
tidle-ms = 15000
poll-after-retransmission = no
repeat-ustat = no
ustat-rsp-to-poll = no
```

## R

### rad-acct-client

**Description** A subprofile that defines how the Stinger unit interacts as a client to RADIUS accounting servers.

**Usage** Following is a listing of the rad-acct-client subprofile with its default settings:

```
[in EXTERNAL-AUTH:rad-acct-client (new)]
acct-server-1 = 0.0.0.0
acct-server-2 = 0.0.0.0
acct-server-3 = 0.0.0.0
acct-port = 0
acct-src-port = 0
acct-key = ""
acct-timeout = 1
acct-sess-interval = 0
acct-id-base = acct-base-10
acct-reset-time = 0
acct-checkpoint = 0
acct-checkpoint-timer = all-sessions
acct-stop-only = yes
acct-limit-retry = 0
acct-drop-stop-on-auth-fail = no
acct-radius-compat = old-ascend
tunnel-accounting = no
```

**See Also** rad-auth-client, rad-auth-server, tac-auth-client, tacplus-auth-client



## rad-auth-client

**Description** A subprofile that defines how the Stinger unit interacts as a client to RADIUS authentication servers.

**Usage** Following is a listing of the rad-auth-client subprofile with its default settings:

```
[in EXTERNAL-AUTH:rad-auth-client]
auth-server-1=0.0.0.0
auth-server-2=0.0.0.0
auth-server-3=0.0.0.0
auth-port=0
auth-src-port=0
auth-key=""
auth-timeout=0
auth-rsp-required=no
auth-sess-interval=0
auth-ts-secure=yes
auth-reset-time=0
auth-Send67=yes
auth-fm-adr-start=no
auth-id-fail-return-busy=no
auth-id-timeout-return-busy=no
auth-radius-compat=old-ascend
auth-keep-user-name=change-name
auth-realm-delimiters="@/\%"
id-auth-prefix=""
allow-auth-config-rqsts=yes
```

## rad-auth-server

**Description** A subprofile that defines how Remote Authentication Dial-In User Service (RADIUS) clients interact with the Stinger unit. With the appropriate software, clients can issue RADIUS commands for session termination and filter changes.

**Usage** Following is a listing of a rad-auth-server subprofile with its default settings:

```
[in EXTERNAL-AUTH:rad-auth-server (new)]
auth-port = 0
auth-session-key = no
auth-attribute-type = rad-serv-attr-any
auth-client = [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 +
auth-netmask = [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 +
auth-key = ["" "" "" "" "" "" "" "" ""]
auth-radius-compat = old-ascend
```

**See Also** rad-acct-client, rad-auth-client, tac-auth-client, tacplus-auth-client

## REDUNDANCY

**Description** A profile that enables you to configure redundant control modules.

**Usage** Following is a listing of the redundancy profile with its default settings:

```
[in REDUNDANCY (new)]
context = [{ } { }]
primary-preference = no-preference
```

## REDUNDANCY-STATS

**Description** A profile that contains the control module redundancy context statistics.

**Usage** Following is a listing of the read-only redundancy-stats profile:

```
[in REDUNDANCY-STATS]
context-stats = [{ monitoring secondary defer-to-running-primary primary +
```

## relay-agent-information

**Description** A subprofile that enables you to configure DHCP option 82, the relay agent information option, by associating a unique identifier with a broadband device such as a DSL CPE or Integrated Access Device (IAD).

**Usage** Following is a listing of the relay-agent-information subprofile with its default settings:

```
[in IP-GLOBAL:bootp-relay:relay-agent-information]
circuit-id = { no 0.0.0.0 }
remote-id = { no 0.0.0.0 }
```

## remote-id

**Description** A subprofile that enables you to configure settings for the remote identifier suboption of DHCP option 82.

**Usage** Following is a listing of the remote-id subprofile with its default settings:

```
[in IP-GLOBAL:bootp-relay:relay-agent-information:remote-id]
enable = no
if-ip = 0.0.0.0
dhcp-allow-any-src-port = no

[in BRIDGE-GROUP/0:dhcp-snooping:remote-id (new)]
enable = no
if-ip = 0.0.0.0
vendor-option-string = ""
version = 1
dhcp-allow-any-src-port = no
```

```
[in BRIDGE-GROUP/0:pppoe-snooping:remote-id (new)]
enable = no
if-ip = 0.0.0.0
vendor-option-string = ""
version = 1
dhcp-allow-any-src-port = no
```

## remote-shelf-config

**Description** A subprofile for enabling and configuring each remote shelf in service on the host system.

**Usage** Following is a listing of the remote-shelf-config profile shown with default values for the remote shelf with shelf-ID 3:

```
[in REMOTE-SHELF-CONFIG/shelf-3]
remote-shelf-id* = shelf-3
enabled = no
name = ""
location = ""
remote-shelf-type = stngr-cascaded-mrt
```

**Dependencies** The remote-shelf-config profile can only be created if shelf-controller-type is set to master.

**See Also** shelf-controller-type

## remote-shelf-stat

**Description** The remote-shelf-stat resides on the host for monitoring remote shelves. This profile is read-only and can not be deleted by a user.

**Usage** Following are the read-only fields in a profile for shelf 3:

```
[in REMOTE-SHELF-STAT/shelf-3]
remote-shelf-id* = shelf-3
host-port = { { any-shelf any-slot 0 } 0 }
remote-shelf-oper-state = remote-shelf-oper-state-up
name = MyShelfName
location = MyShelfLocation
internal-fan-unit-failed = no
external-fan-unit-failed = no
door-open = no
over-temperature = no
contact-closure = [no no no no no no no]
topology = { remote-shelf-cascade-port-none any-shelf any-shelf }
validation-status = { no 0 0 }
```

## rlogin-options

**Description** *Not used.*

**Location** `TERMINAL-SERVER:terminal-mode-configuration`

## route-description-list [n]

**Description** A subprofile that defines a route to be included in the private routing table. Specific connection or RADIUS profiles can refer to a private routing table by name to have access to its routes.

**Usage** Set values in this subprofile to configure one of up to 24 routes. Following is a listing of a route-description-list subprofile with its default settings:

```
[in PRIVATE-ROUTE-TABLE/":route-description-list[1]]
enabled = no
dest-address = 0.0.0.0/0
netmask = 0.0.0.0
gateway-address = 0.0.0.0
metric = 0
```

## route-filter

**Description** An input-filter or output-filter subprofile for defining a packet filter to be applied to RIP updates.

**Usage** Set values in this subprofile to configure one of up to 12 input or output route filters. Following are sample route-filter listings:

```
[in FILTER/":input-filters[1]:route-filter]
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
route-mask = 0.0.0.0
route-address = 0.0.0.0
add-metric = 0
action = none

[in FILTER/":output-filters[1]:route-filter]
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
route-mask = 0.0.0.0
route-address = 0.0.0.0
add-metric = 0
action = none
```

## rxlink-config

**Description** A subprofile that enables you to configure the receiving link in an inverse multiplexing over ATM (IMA) connection.

**Usage** Following is a listing of an rxlink-config subprofile.

```
[in DS1-ATM/{ any-shelf any-slot 0 }:line-config:ima-option-config:
rxlink-config]
add-link-cond-time = 3
link-recovery-type = fast
rec-link-cond-time = 10
rx-lid-learning-time = 100
fault-clearing-type = auto
fault-clearing-time = 10
in-defect-int-time = 2500
out-defect-int-time = 10000
defect-ratio = 10
```

## S

### scheduling

**Description** Specifies a scheduling priority.

**Usage** Following is a listing of the scheduling profile shown with default settings:

```
[in PACKET-FLOWS/"" :flow[1] :scheduling (new)]
queue-priority = 0
```

### SDSL

**Description** A profile containing configuration settings for an SDSL line interface module (LIM).

**Usage** Following is a listing of the sdsl profile with its default settings:

```
[in SDSL/{ shelf-1 slot-1 0 }]
name=""
physical-address*={ shelf-1 slot-1 0 }
enabled=no
sparing-mode = inactive
line-config={ 0 0 static { any-shelf any-slot 0 } }
```

### SDSL-STAT

**Description** A read-only profile that indicates the status of the SDSL line.

**Usage** Read-only. Following is a sample listing of the sdsl-stat profile:

```
[in SDSL-STAT/{ shelf-1 slot-13 20 }]
physical-address* = { shelf-1 slot-13 20 }
line-state = disabled
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
error-count = 0
physical-status = { 0 coe out-of-service 0 0 0 0 0 }
physical-statistic = { { 0 0 0 } no 0 0 passed 0 idle 0 }
```

## security-properties

**Description** A subprofile that enables you to configure the security model and name for a view-based access control model (VACM).

**Usage** Following is a listing of the security-properties subprofile with its default settings:

```
[in VACM-SECURITY-GROUP/{ v1 "" }:security-properties (new)]
security-model = v1
security-name = ""
```

## SERIAL

**Description** A profile that specifies physical interface settings for a system serial interface.

**Usage** Following is a listing of the serial profile with its default settings:

```
[in SERIAL/{ any-shelf any-slot 0 } (new)]
physical-address* = { any-shelf any-slot 0 }
term-rate = 9600-bps
flow-control = none
user-profile = admin
auto-logout = no
console-mode = on
```

## service-options

**Description** A flow-list subprofile for defining service-specific parameters applicable to the layer 2 traffic flow.

**Usage** Following is a listing of the service-options profile shown with default settings:

```
[in FLOW-SERVICES/"" :flow-list[1] :service-options (new)]
vlan-id = 0
```

## session-info

**Description** A subprofile that enables you to configure settings for established sessions. Set values in this subprofile to affect default time-outs, or to set default filters for RADIUS-authenticated profiles.

**Usage** Following is a listing of the session-info subprofile with its default settings:

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

**Dependencies** If the same value is set in a connection profile, the connection-specific setting is used.

## session-options

**Description** A subprofile that enables you to configure settings for an established session.

**Usage** Following is a listing of the session-options subprofile with its default settings:

```
[in CONNECTION/"":session-options]
call-filter = ""
data-filter = ""
filter-persistence = no
filter-required = no
flow-services = ""
idle-timer = 120
ts-idle-mode = no-idle
ts-idle-timer = 120
backup = ""
max-call-duration = 0
ses-rate-type = disabled
ses-rate-mode = autobaud
ses-sdsl-rate = 784000
ses-adsl-dmt-up-rate = 928000
ses-adsl-dmt-down-rate = 8000000
traffic-shaper = 16
```

## shdsl

**Description** A profile that enables you to configure settings for SHDSL LIMs.

**Usage** Following is a listing of the shdsl profile with its default settings:

```
[in SHDSL/{ any-shelf any-slot 0 } (new)]
name = ""
physical-address* = { any-shelf any-slot 0 }
enabled = no
sparing-mode = inactive
ignore-lineup = system-defined
line-config = { 0 1 15 static { any-shelf any-slot 0 } coe no not-eligible +
```

## SHDSL-STAT

**Description** A read-only profile that indicates the status of each SHDSL interface. The Stinger unit creates an shdsl-stat profile for each SHDSL interface in the system.



**Usage** Following is a listing of the shdsl profile with sample settings for an active line:

```
[in SHDSL-STAT/{ shelf-1 slot-2 10 }]
physical-address* = { shelf-1 slot-2 10 }
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 = { 0 cpe port-up 1544000 A100 1 }
physical-statistic = { { 0 0 3 } yes 36 3 passed 10 0 in-sync 0 0 0 0 0 no+
```

## slip-mode-configuration

**Description** *Not used.*

**Location** `TERMINAL-SERVER`

## SLOT-ADMIN

**Description** A profile that enables you to specify the operational state of the module in a particular slot.

**Usage** Following is a listing of the slot-admin profile with its default settings:

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

## SLOT-INFO

**Description** A read-only profile that displays the software version, serial number, and other system information about the Stinger unit.

**Usage** Read-only. Following is a sample listing of the slot-info profile. Use the Get command to display the listing.

```
[in SLOT-INFO]
slot-address={ shelf-1 slot-7 0 }
serial-number=77777777
software-version=1
software-revision=2
software-level=E
software-release=""
hardware-level=0
```

## SLOT-STATE

**Description** A read-only profile that indicates the current state of a slot module. The slot-state profile does not reside in nonvolatile RAM (NVRAM), so it does not persist across system resets or power cycles. Simple Network Management Protocol (SNMP) managers can read the slot-state profile.

**Usage** Following is a sample listing of the slot-state profile:

```
[in SLOT-STATE/{ shelf-1 slot-2 0 }]
slot-address*={ shelf-1 slot-2 0 }
current-state=oper-state-none
```

## SLOT-STATIC-CONFIG

**Description** A profile that enables you to configure additional per-slot static parameters. There is one slot-static-config profile available for each line interface module (LIM) and control module slot. This profile can not be deleted by a user.

**Usage** Following is a listing of the slot-static-config profile with its default settings:

```
[in SLOT-STATIC-CONFIG/{ any-shelf any-slot 0 }]
name = ""
physical-address* = { any-shelf any-slot 0 }
atm-parameters = { low-priority }
interface-type = default
use-vp-switching-workaround = no
need-max-vpswitching-vpis = no
adsl-card-annex-type = annex-c
prof-update = no
vpi-vci-range = vpi-0-15-vci-32-127
allow-max-up-stream-bandwidth = 1000
allow-guaranteed-up-stream-bandwidth = 0
port-cac-enable = no
port-over-subscription = 10
slot-cac-enable = yes
slot-over-subscription = 10
num-of-vci = two-k
```

## SLOT-TYPE

**Description** A read-only profile that stores information about the type of slot card installed in each shelf/slot location. The slot-type profile resides in nonvolatile RAM (NVRAM) and persists over system resets.

**Usage** Read-only. Following is a sample listing of the slot-type profile.

```
[in SLOT-TYPE/{ shelf-1 slot-8 0 }]
slot-address*={ shelf-1 slot-8 0 }
slot-type=sdsl-card
```

## slot-vpi-vci-range

**Description** *Deprecated and not used.*

**Location** ATM-CONFIG

**See Also** SLOT-STATIC-CONFIG

## SNMP

**Description** A profile configures settings that determine Simple Network Management Protocol (SNMP) security, specify a contact and location, and control which hosts can access the Stinger unit by means of the SNMP manager utilities.

**Usage** Following is a listing of the `snmp` profile with its default settings:

```
[in SNMP (new)]
enabled = yes
read-community = *****
read-write-enabled = yes
read-write-community = *****
enforce-address-security = no
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 +
write-access-hosts = [0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 +
contact = ""
location = ""
queue-depth = 0
csm-modem-diag = no
engine-id = 00:00:00:00:00:00:00:00:00:00:00
engine-boots = 0
snmp-message-type = v1-and-v3
security-level = none
enable-vacm = no
notification-log-age-out = 1440
bit-strings-allowed = yes
```

## SNMP-MANAGER

**Description** A profile that enables you to configure the security hosts of the Simple Network Management Protocol (SNMP) manager.

**Usage** Following is a listing of the `snmp-manager` profile with its default settings:

```
[in SNMP-MANAGER/"" (new)]
name* = ""
active = no
write-access = no
snmp-message-type = v1-and-v3
```

## SNMPV3-NOTIFICATION

**Description** A profile that, in conjunction with the `snmpv3-target-params` profile, configures 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 user names.

**Usage** Following is a listing of the `snmpv3-notification` profile with its default settings:

```
[in SNMPV3-NOTIFICATION/default]
name* = default
active-enabled = yes
tag = default
type = trap
```

**See Also** `SNMPV3-TARGET-PARAM`

## SNMPV3-TARGET-PARAM

**Description** A profile that, in conjunction with the `snmpv3-notification` profile, configures 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 notification feature follows the specifications in RFC 2573.

**Usage** Following is a listing of the `snmpv3-target-params` profile with its default settings:

```
[in SNMPV3-TARGET-PARAM/default]
name* = default
active-enabled = yes
msg-proc-model = v1
security-model = v1
security-name =
security-level = none
```

**See Also** `SNMPV3-NOTIFICATION`

## SNMPV3-USM-USER

**Description** A profile that permits you to create and edit user profiles for support of SNMPv3 user-based security model (USM) privacy.

**Usage** Following is a listing of the `snmpv3-usm-user` profile with its default settings:

```
[in SNMPV3-USM-USER/groupz]
name* =groupz
active-enabled = no
read-write-access = no
auth-protocol = md5-auth
priv-protocol = no-priv
auth-key =
priv-key =
public-str = ""
```

## sntp-info

**Description** A subprofile that enables you to configure the use of the Simple Network Time Protocol (SNTP), which is described in RFC 1305.

**Usage** Following is a listing of the `sntp-info` subprofile with its default settings:

```
[in IP-GLOBAL:sntp-info]
enabled = sntp-disabled
GMT-offset = utc+0000
host = [0.0.0.0 0.0.0.0 0.0.0.0]
update-threshold = 10
```

## SONET

**Description** A profile that enables you to configure settings for an OC12-ATM SONET interface.

**Usage** Following is a listing of the `SONET` profile with its default settings:

```
[in SONET/{ shelf-1 trunk-module-1 1 }]
name = 1:17:1
physical-address* = { shelf-1 trunk-module-1 1 }
enabled = no
ignore-lineup = system-defined
aps-config-name =
line-config = { 0 851 payload-atm no-loopback sonet no no vpi-0-255-vci-32-8191+
atm-config = { ast-x43 ast-x43 yes }
spare-physical-address = { any-shelf any-slot 0 }
sparing-mode = inactive
```

## SONET-STAT

**Description** A read-only profile that indicates the state of the physical interface, error counters, and ATM framer status for each OC12 interface.

**Usage** Read-only. Following is a sample listing of a SONET-STAT profile:

```
[in SONET-STAT/{ shelf-1 trunk-module-1 1 }]
physical-address* = { shelf-1 trunk-module-1 1 }
line-state = active
line-rate = OC-12c
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 0 0 0 0 0 0 0 0 0 0 0 0]
aps-config-name = ""
aps-channel-status = unknown
aps-channel-sd-condition = False
aps-channel-sf-condition = False
aps-channel-low-direction = low-none
aps-channel-recv-sd-count = 0
aps-channel-recv-sf-count = 0
aps-channel-recv-ais-count = 0
aps-channel-recv-rdi-count = 0
loss-of-signal = False
loss-of-frame = False
out-of-frame = False
section-state = sonet-section-active-no-defect
path-state = sonet-path-active-no-defect
ais-receive = False
yellow-receive = False
out-of-cell-delineation = False
loss-of-cell-delineation = False
aps-receive = False
rsop-bip-error-count = 46350
rlop-bip-error-count = 52896
rlop-febe-error-count = 0
rpop-bip-error-count = 0
rpop-febe-error-count = 0
racp-chcs-error-count = 0
racp-uchcs-error-count = 0
racp-rx-cell-count = 0
tacp-tx-cell-count = 0
frequency-justification-count = 0
HEC-cell-drop-counter = 0
FIFO-overflow-counter = 0
idle-cell-counter = 0
valid-cell-counter = 0
short-packet-counter = 0
bad-crc-packet-counter = 0
bad-seq-packet-counter = 0
valid-packet-counter = 0
time-elapsed = 743
valid-intervals = 79
```

```
performance-monitoring = { 646 664 0 46350 0 0 0 664 0 0 0 0 0 0 0 0 0 0 }
interval-performance-monitoring = [{ 876 901 0 7323 0 0 0 901 0 0 0 0 0 0 0 0 +
spare-physical-address = { any-shelf any-slot 0 }
sparing-state = sparing-none
sparing-change-reason = unknown
sparing-change-time = 0
sparing-change-counter = 0
```

## spvc-address-prefix

**Description** A subprofile of the atm-prefix profile that contains the prefix portion of the SPVC target address.

**Usage** Following is a listing of the spvc-address-prefix subprofile with its default settings:

```
[in ATM-PREFIX/default:spvc-address-prefix]
length = 0
address = 00:00:00:00:00:00:00:00:00:00:00:00
```

## svc-addr-prefix

**Description** A subprofile that contains the prefix portion of the SVC target address

**Usage** Following is a listing of the svc-addr-prefix subprofile with its default settings:

```
[in ATM-PREFIX/default:svc-addr-prefix]
length = 0
address = 00:00:00:00:00:00:00:00:00:00:00:00
```

**See Also** pnmi-node-prefix, spvc-addr-prefix

## SWITCH-CONFIG

**Description** A profile that enables you to configure an Asynchronous Transfer Mode (ATM) application-specific integrated circuit (ASIC). This profile is indexed by the module on which the ASIC is located (for example, controller, tram-17, or tram-18). The system creates a profile for the controller ASIC. If a trunk aggregation module (TRAM) is installed, it also creates a switch-config profile for those processors.

**Usage** Following is a listing of the switch-config profile with its default settings:

```
[in SWITCH-CONFIG/controller]
switch-name* = controller
atm-parameters = { [{ yes 1:17:1 { shelf-1 trunk-module-1 1 } yes no +
```

**See Also** atm-parameters

## SYSTEM

**Description** A profile that enables you to configure systemwide settings for call management.

**Usage** Following is a listing of the system profile with its default settings:

```
[in SYSTEM]
installation-complete = yes
name = idslstg
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 = 9.2-167.1
system-8k-clock = controller
ignore-lineup = no
nvram-was-rebuilt = no
connection-profile-auto-naming-convention = lower-interface-number-first
cac-preference = connection-time
traffic-shapers = [{ no 0 0 2 no 1 } { no 0 0 2 no 2 } { no 0 0 2 no 3 } { +
validation-enable = yes
user-second-level-authentication = none
maximum-login-attempts = 3
audit-user-profiles = yes
atm-qos-rate-unit = kbps
np-update-time = 0
np-default-filtering-policy = forward
```

## SYSTEM-INTEGRITY

**Description** A profile for internal use only.



# T

## T1-STAT

**Description** A read-only profile that displays information about the state of a T1 line and its channels.

**Usage** Read-only. Following is a sample listing of a `t1-stat` profile:

```
[in T1-STAT/{ shelf-1 slot-1 1 }]
physical-address* = { shelf-1 slot-1 1 }
line-state = disabled
channel-state = [disabled disabled disabled disabled disabled disabled disabled+
error-count = [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
loss-of-carrier = False
loss-of-sync = False
ais-receive = False
yellow-receive = False
ber-receive = False
carrier-established = False
network-loopback = False
```

## table-config

**Description** A subprofile that enables you to configure the Domain Name System (DNS) local table, storing up to eight host names and initial IP addresses.

**Usage** Following is a sample listing of the `table-config` subprofile:

```
[in IP-GLOBAL:dns-local-table:table-config[1]]
host-name = ""
ip-address = 0.0.0.0
```

## tac-auth-client

**Description** A subprofile that enables you to configure the way in which a Stinger unit interacts as a client of Terminal Access Controller Access Control System (TACACS) protocol authentication servers.

**Usage** Following is a listing of the `tac-auth-client` subprofile with its default settings:

```
[in EXTERNAL-AUTH:tac-auth-client]
auth-server-1 = 0.0.0.0
auth-server-2 = 0.0.0.0
auth-server-3 = 0.0.0.0
auth-port = 0
auth-src-port = 0
auth-key = ""
auth-timeout = 0
```

## tacplus-acct-client

**Description** A subprofile that defines how the Stinger unit interacts as a client of TACACS+ accounting servers.

**Usage** Following is a listing of a tacplus-acct-client subprofile with its default settings:

```
[in EXTERNAL-AUTH:tacplus-acct-client (new)]
acct-server-1 = 0.0.0.0
acct-server-2 = 0.0.0.0
acct-server-3 = 0.0.0.0
acct-port = 0
acct-src-port = 0
acct-key = ""
```

## tacplus-auth-client

**Description** A subprofile that defines how the Stinger unit interacts as a client of TACACS+ authentication servers.

**Usage** Following is a listing of a tacplus-auth-client subprofile with its default settings:

```
[in EXTERNAL-AUTH:tacplus-auth-client (new)]
auth-server-1 = 0.0.0.0
auth-server-2 = 0.0.0.0
auth-server-3 = 0.0.0.0
auth-port = 0
auth-src-port = 0
auth-key = ""
auth-timeout-time = 0
auth-retries = 0
```

## tacl

**Description** Configure restrictions for telnet access.

**Usage** Following is a listing of the tacl profile shown with default settings:

```
[in TACL (new)]
enable-permit = no
permit-list = [{ no 0.0.0.0/0 0.0.0.0 } { no 0.0.0.0/0 0.0.0.0 } { no 0.0.
```

## tcp-clear-answer

**Description** *Not supported.* A subprofile that enables TCP-Clear sessions.

**Usage** Following is a listing of the tcp-clear-answer subprofile, which is not supported in Stinger units.

```
[in ANSWER-DEFAULTS:tcp-clear-answer]
enabled = yes
```

## tcp-clear-options

**Description** *Not supported.* A subprofile that enables you to configure default settings for a TCP-Clear session.

**Usage** Following is a listing of the tcp-clear-options subprofile, which is not supported in Stinger units.

```
[in CONNECTION/":tcp-clear-options (new)]
host = ""
port = 0
host2 = ""
port2 = 0
host3 = ""
port3 = 0
host4 = ""
port4 = 0
detect-end-of-packet = no
end-of-packet-pattern = ""
flush-length = 256
flush-time = 20
```

## tdr-distance-level

**Description** A subprofile that contains distance and level data pairs for the time-domain reflectometry (TDR) test of the copper loop test (CLT) module.

**Usage** Following is a listing of the subprofile with its defaults.

```
[in CLT-RESULT:tdr-distance-level [1]]
distance = 0
level = 0
```

## telco-options

**Description** A subprofile that enables you to configure options negotiated with the telephone company carrier.

**Usage** Following is a listing of the telco-options subprofile with its default settings:

```
[in CONNECTION/":telco-options (new)]
answer-originate = ans-and-orig
callback = no
call-type = ft1
nailed-groups = 1
nailed-up-group = 1
ft1-caller = no
force-56kbps = no
data-service = 56k-clear
call-by-call = 0
billing-number = ""
transit-number = ""
expect-callback = no
delay-callback = 0
nas-port-type = any
```

## telnet-options

**Description** *Not used.*

**Location** `TERMINAL-SERVER:terminal-mode-configuration`

## terminal-mode-configuration

**Description** *Not used.*

**Location** `TERMINAL-SERVER`

## TERMINAL-SERVER

**Description** *Not used.*

**Location** `TERMINAL-SERVER`

## THERMAL

**Description** *Not supported.* A profile that enables you to specify temperature thresholds for the built-in temperature sensors in the Stinger control module.

**Usage** Following is a listing of the thermal profile with its default settings:

```
[in THERMAL]
bottom-low-temperature-threshold = 0
bottom-high-temperature-threshold = 60
top-low-temperature-threshold = 0
top-high-temperature-threshold = 60
```

**Dependencies** Temperature sensors are available only in version 3 and higher of the control module.

## THRESH-HDSL2-SHDSL

**Description** *Not supported.*

## thresh-profiles

**Description** *Not supported.*

**Location** HDSL2

## time

**Description** A subprofile that specifies the current hour, minute, and second.

**Usage** Following is a sample listing of the time subprofile:

```
[in TIMEDATE:time]
hour = 12
minute = 37
second = 33
```



**Note** As an alternative, you can use the set command—for example, set time hour=16. You can also use the date command to set the current hour, minute, and second.

## TIMEDATE

**Description** A profile that shows the current system time and date.

**Usage** Following is a sample listing of the timedate profile:

```
[in TIMEDATE]
time = { 12 37 33 }
date = { Friday March 29 2002 }
```

## tns-index

**Description** A subprofile that specifies a complex index value identifying the transit network selection (TNS). The index elements are defined in the subprofile.

**Usage** Following is a listing of the tns-index subprofile:

```
[in PNNI-ROUTE-TNS/{ 0 other other "" 0 }:tns-index]
node-index = 0
route-tns-type = other
route-tns-plan = other
route-tns-id = ""
route-tns-index = 0
```

## tos-filter

**Description** An input-filter or output-filter subprofile for defining a type of service (ToS) filter.

**Usage** Set values in this subprofile to configure one of up to 12 input or output ToS filters. Following are sample tos-filter listings:

```
[in FILTER/":input-filters[1]:tos-filter]
protocol = 0
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
dest-address-mask = 0.0.0.0
dest-address = 0.0.0.0
Src-Port-Cmp = none
source-port = 0
Dst-Port-Cmp = none
dest-port = 0
precedence = 000
type-of-service = normal
marking-type = precedence-tos
dscp = 00

[in FILTER/":output-filters[1]:tos-filter]
protocol = 0
source-address-mask = 0.0.0.0
source-address = 0.0.0.0
dest-address-mask = 0.0.0.0
dest-address = 0.0.0.0
Src-Port-Cmp = none
source-port = 0
Dst-Port-Cmp = none
dest-port = 0
precedence = 000
type-of-service = normal
marking-type = precedence-tos
dscp = 00
```

## tos-options

**Description** A subprofile that enables you to configure type-of-service (TOS) settings for IP routed WAN connections. Stinger units do not implement priority queuing, but they do set information that can be used by other routers to prioritize and select links for particular data streams. You set values in this subprofile to configure the Stinger unit to set quality of service (QoS) priority bits and TOS classes of service on behalf of customer applications.

**Usage** Following is a listing of the `tos-options` subprofile with its default settings:

```
[in CONNECTION/":ip-options:tos-options]
active = no
precedence = 000
type-of-service = normal
apply-to = incoming
marking-type = precedence-tos
dscp = 00
```

**See Also** `ip-options`

## traffic-shapers

**Description** A subprofile that enables you to configure the bandwidth of virtual circuits.

**Usage** Following is a listing of a `traffic-shapers` subprofile with its default settings:

```
[in ATM-CONFIG:traffic-shapers[1]]
enabled = no
bit-rate = 1000
peak-rate = 1000
max-burst-size = 2
aggregate = no
priority-number = 1
```

## transceiver-info

**Description** A read-only subprofile that identifies the interface and the type of transceiver in the trunk card.

**Usage** Following is a listing of the `transceiver-info` profile:

```
[in TRUNK-DAUGHTER-DEV/{ shelf-1 trunk-module-1 1 }:transceiver-info]
reach-type = long-reach
interface-type = interface-oc12
```

## TRAP

**Description** A profile that enables you to configure the way in which the Stinger unit traps events. A trap is a mechanism in Simple Network Management Protocol (SNMP) for reporting system change in real time. To report system change, the Stinger unit sends a traps-PDU (protocol data unit) to the SNMP manager. (For the most up-to-date information about events, see the Ascend Enterprise MIB.)

**Usage** Following is a listing of the trap profile with its default settings:

```
[in TRAP/" (new)]
host-name* = ""
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
trap-sequencing = no
heart-beat-trap-interval = 5
trap-optimization-enabled = no
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-config-error-enabled = no  
ospf-virt-if-auth-failure-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  
hdl2-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  
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  
remote-shelf-enabled = yes  
trap-shelf-clli = no

## tree-properties

**Description** A subprofile that enables you to configure the identifiers of a view in a view-based access control model (VACM).

**Usage** Following is a listing of the tree-view-properties subprofile with its default settings:

```
[in VACM-VIEW-TREE/{ "" "" }:tree-properties (new)]
view-name = ""
view-tree-oid = ""
```

**See Also** trunk-cac-config[n]

## trunk-cac-config

**Description** A subprofile of the high-speed-slot profile that the system creates for each trunk port.

**Usage** Following is a listing of a trunk-cac subprofile with its default settings:

```
[in HIGH-SPEED-SLOT-STATIC-CONFIG/{ shelf-1 trunk-module-1 1 }:trunk-cac-
config]
enable = yes
port-num = 1:17:1
line-rate = 148598
over-subscription = 10
```

**Dependencies** This parameter was previously located in the atm-config profile. Its use in that location has been deprecated.

If a user has already set these parameters under a previous release in the atm-config profile, the parameters are copied into the corresponding high-speed-slot-static-config profile. The parameters are now invisible in the atm-config profile unless allow-debug is set to yes.

## trunk-cac-config [n]

**Description** *Deprecated and not used.*

**Location** ATM-CONFIG:trunk-cac-config

**See Also** HIGH-SPEED-SLOT-STATIC-CONFIG

## TRUNK-DAUGHTER-DEV

**Description** A profile that enables you to configure a trunk daughter device.

**Usage** Following is a listing of the trunk-daughter-dev profile:

```
[in TRUNK-DAUGHTER-DEV/{ shelf-1 trunk-module-2 1 }]
device-address* = { shelf-1 trunk-module-2 1 }
device-state = trunk-daughter-oper-state-up
trunk-daughter-type = trunk-daughter-oc3-quad
previous-trunk-daughter-type = trunk-daughter-none
transceiver-info = { long-reach interface-oc12 }
```

## tunnel-options

**Description** A subprofile configures virtual private network (VPN) connectivity using Layer 2 Tunneling Protocol (L2TP) or Ascend Tunnel Management Protocol (ATMP) tunneling.

**Usage** Following is a listing of the tunnel-options subprofile with its default settings:

```
[in CONNECTION/":tunnel-options]
profile-type = disabled
tunneling-protocol = atmp-protocol
max-tunnels = 0
atmp-ha-rip = rip-off
primary-tunnel-server = ""
secondary-tunnel-server = ""
udp-port = 5150
password = ""
home-network-name = ""
client-auth-id = ""
server-auth-id = ""
vrouter = ""
assignment-id = ""
```

**Dependencies** RADIUS-authenticated PPP sessions can use some L2TP tunnel features, such as tunnel tags, that are not supported in the local command-line interface.

## TUNNEL-SERVER

**Description** A profile that enables you to configure server-level tunnel authentication and other options specific to a Layer 2 Tunneling Protocol (L2TP) network server (LNS).

**Usage** Following is a listing of the tunnel-server profile with its default settings:

```
[in TUNNEL-SERVER/""]
server-endpoint* = ""
enabled = yes
shared-secret = ""
client-auth-id = ""
server-auth-id = ""
dialout-options = { no "" "" "" "" no no }
```

**See Also** dialout-options

## txlink-config

**Description** A subprofile that enables you to configure the transmitting link in an inverse multiplexing over ATM (IMA) connection.

**Usage** Following is a sample listing of the txlink-config subprofile:

```
[in DS1-ATM/{ shelf-1 any-slot 0 }:line-config:ima-option-config:txlink-
confi+
ne-tx-lid = 0
add-link-cond-time = 3
link-recovery-type = fast
fault-clearing-type = auto
fault-clearing-time = 10
priority = 0
```

**See Also** ima-option-config, line-config

## U

### USER

**Description** A profile that defines a name, a password, privileges, and default displays for user login accounts.

**Usage** Following is a listing of a user profile with its default settings:

```
[in USER/default]
name*=default
password=""
active-enabled=yes
enforce-password-check = no
first-level-user = ""
login-level = first-level
allow-termserv=no
allow-system=no
allow-diagnostic=no
allow-update=no
allow-password=no
allow-code=no
idle-logout=0
prompt="admin> "
default-status=no
top-status=general-info
bottom-status=log-window
left-status=connection-list
use-scroll-regions=yes
log-display-level=none
screen-length=24
status-length=18
user-group = ""
last-login-date = { Wednesday November 2003 12 }
user-acct-expiration-date = { Saturday November 2006 11 }
user-passwd-expiration-date = { Sunday January 2004 11 }
```

user-group

**Description** The user-group profile enables you to define command access for each user you specify. You can specify access settings and a list of up to 512 commands that users in the command user group have permission to use.

**Usage** Following are the parameters, shown with their default settings:

[illegible]

## usrrad-options

**Description** A subprofile that enables you to configure connection-specific RADIUS accounting options.

**Usage** Following is a listing of the `usrrad-options` subprofile with its default settings:

```
[in CONNECTION/tim:usrRad-options]
acct-type=global
acct-host=0.0.0.0
acct-port=1646
acct-key=""
acct-timeout=1
acct-id-base=acct-base-10
```

**Dependencies** RADIUS accounting must be configured in the `rad-acct-client` subprofile of the `external-auth` profile.

## V

### VACM-ACCESS

**Description** A profile that enables you to configure the view-based access control model (VACM), specifying view names for different kinds of access, such as read, write, notify.

**Usage** Following is a listing of the vacm-access profile with its default settings:

```
[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 = ""
```

### VACM-SECURITY-GROUP

**Description** A profile that enables you to configure the mapping of a security name and security model in an incoming or outgoing message to a view-based access control model (VACM) security group.

**Usage** Following is a listing of the vacm-security-group profile with its default settings:

```
[in VACM-SECURITY-GROUP/{ v1 "" } (new)]
security-properties* = { v1 "" }
active = no
group-name = ""
```

### VACM-VIEW-TREE

**Description** A profile that enables you to configure the views of the view-based access control model (VACM).

**Usage** Following is a listing of the vacm-view-tree profile with its default settings:

```
[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
```

## validation-status

**Description** Validation status of the remote shelf.

**Usage** Following are the read-only fields in a profile for shelf 3:

```
[in REMOTE-SHELF-STAT/shelf-3:validation-status]
id-valid = disabled
validation-id-setting = 0
validation-id = 0
```

## vcc-ident

**Description** A read-only subprofile that indicates values for a virtual channel connection (VCC) on an Asynchronous Transfer Mode (ATM) link.

**Usage** Read-only. Following is a listing of the vcc-ident subprofile with sample

```
[in ATMVCC-STAT/{ shelf-1 slot-1 3 0 41 1 }:vcc-ident]
shelf-number = shelf-1
slot-number = slot-1
port = 3
vpi = 0
vci = 41
nailed-group = 1
```

## vcc-members

**Description** A read-only subprofile that indicates the values for the virtual channel connections (VCCs) on an Asynchronous Transfer Mode (ATM) link.

**Usage** Read-only. Following is a sample listing of the vcc-members subprofile:

```
[in ATMPVC-STAT/unit1:vcc-members]
vcc-members[1]={ shelf-1 slot-2 14 0 37 }
vcc-members[2]={ shelf-1 trunk-module-2 2 0 10
```

## vcc-members [n]

**Description** A read-only subprofile of the atmpvc-stat:vcc-members subprofile that contains values for a virtual channel connection (VCC) on an Asynchronous Transfer Mode (ATM) link.

Following is a sample listing of the vcc-members n subprofile:

```
[in ATMPVC-STAT/unit1:vcc-members[1]]
shelf-number = shelf-1
slot-number = trunk-module-1
port = 1
vpi = 0
vci = 120
nailed-group = 801
```



## VLAN-ETHERNET

**Description** A profile that enables you to specify the configuration of IEEE 802.1Q virtual local area networks (VLANs).

**Usage** Following is a listing of the vlan-ethernet profile with its default settings:

```
[in VLAN-ETHERNET/{ { any-shelf any-slot 0 } 0 } (new)]
interface-address* = { { any-shelf any-slot 0 } 0 }
vlan-enabled = no
vlan-id = 0
enabled = no
filter-name = ""
pppoe-options = { no no }
bridging-options = { 0 no no }
```

## VRROUTER

**Description** A profile that defines a virtual router (VRouter).

**Usage** Following is a listing of the vrouter profile with its default settings:

```
[in VRROUTER/""]
name* = ""
active = yes
vrouter-ip-addr = 0.0.0.0
pool-base-address = [0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0+
assign-count = [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 +
pool-name = ["" +
pool-summary = no
pool-chaining = no
share-global-pool = yes
rip-policy = Poison-Rvrs
summarize-rip-routes = no
rip-trigger = yes
domain-name = ""
sec-domain-name = ""
dns-primary-server = 0.0.0.0
dns-secondary-server = 0.0.0.0
client-primary-dns-server = 0.0.0.0
client-secondary-dns-server = 0.0.0.0
allow-as-client-dns-info = True
```

## W

### wan-router-interface-profile

**Description** Name of the connection profile to be used as the “router” port in terms of traffic handling for this bridge group, i.e., the default path for uplinks from users. The specified connection must be on a trunk interface. This setting and the `lan-router-interface-address` setting are mutually exclusive.

**Usage** Following is a listing of the `wan-router-interface-profile` profile shown with default settings:

```
[in BRIDGE-GROUP/0:wan-router-interface-profile (new)]
wan-router-interface-profile = ""
```

**Dependencies** This setting and the `lan-router-interface-address` setting are mutually exclusive.

### WATCHDOG-CONFIG

**Description** A profile that enables you to specify Simple Network Management Protocol (SNMP) traps (notifications) for specific conditions.

**Usage** Following is a listing of the `watchdog-config` profile with sample settings:

```
[in WATCHDOG-CONFIG/{ fan fantray 1 }]
watchdog-index* = { fan fantray 1 }
watchdog-trap-enable = yes
watchdog-name = "Stinger 10 Fan"
system-created-slave-profile = no
```

### watchdog-index\*

**Description** A complex field that contains the watchdog type, location ID, and unit number of a Simple Network Management Protocol (SNMP) *watchdog*. A watchdog is a software routine that monitors the status of a particular aspect of a Stinger unit—for example, the temperature of a module.

**Usage** Following is a listing of the `watchdog-index` field with its default settings:

```
[in WATCHDOG-CONFIG/{ none 0 }:watchdog-index (new)]
watchdog-type = (bad value)
location-id = none
unit = 0
```

# X

## XDSL-SLOT-CONFIG

**Description** A profile that enables you to configure an xDSL slot.

**Usage** Following is a listing of the xdsl-slot-config profile with its default settings:

```
[in XDSL-SLOT-CONFIG/{ any-shelf any-slot 0 }]
slot-address* = { any-shelf any-slot 0 }
sealing-current-on = no
```



---

# Stinger Parameter Reference



3

|               |       |
|---------------|-------|
| Numeric ..... | 3-2   |
| A.....        | 3-5   |
| B.....        | 3-76  |
| C.....        | 3-91  |
| D.....        | 3-133 |
| E.....        | 3-165 |
| F.....        | 3-179 |
| G.....        | 3-203 |
| H.....        | 3-210 |
| I.....        | 3-221 |
| j.....        | 3-249 |
| K.....        | 3-249 |
| L.....        | 3-250 |
| M.....        | 3-281 |
| N.....        | 3-319 |
| O.....        | 3-344 |
| P.....        | 3-358 |
| Q.....        | 3-393 |
| R.....        | 3-396 |
| S.....        | 3-430 |
| T.....        | 3-492 |
| U.....        | 3-533 |
| V.....        | 3-547 |
| W.....        | 3-561 |
| X.....        | 3-565 |
| Y.....        | 3-566 |

## Numeric

32-dmt-aslam

**Description** *Deprecated and not used.*

**Location** LOAD-SELECT

40-dmt-adsl

**Description** *Deprecated and not used.*

**Location** LOAD-SELECT

48-dmt-adsl

**Description** Specifies whether code images for ADSL 48-port line interface modules (LIMs) are to be stored in flash memory.

**Usage** Valid values are as follows:

- **auto**—Causes the system to load images for ADSL 48-port LIMs that are installed in the Stinger unit and to skip images for modules that are not installed. This is the default.
- **load**—Causes the system to load the image, even if no ADSL 48-port LIMs are installed.
- **skip**—Causes the system to skip the image, even if an ADSL 48-port LIM is installed.



**Note** A module is considered present in the system if a `slot-type` profile exists for that module type. The system creates a `slot-type` profile when it first detects the presence of a particular module. The system does not delete the profile unless you use the `slot -r` command to permanently remove a module that is no longer installed in the system, or clear nonvolatile RAM (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.

**Example** `set 48-dmt-adsl = auto`

**Location** LOAD-SELECT

## 72-ct-dmt-adsl

**Description** Specifies whether code images for ADSL 72-port Annex A line interface modules (LIMs) are to be stored in flash memory.

**Usage** Valid values are as follows:

- **auto**—Causes the system to load images for ADSL 72-port Annex A LIMs that are installed in the Stinger unit and to skip images for modules that are not installed. This is the default.
- **load**—Causes the system to load the image, even if no ADSL 72-port Annex A LIMs are installed.
- **skip**—Causes the system to skip the image, even if an ADSL 72-port Annex A LIM is installed.



**Note** A module is considered present in the system if a slot-type profile exists for that module type. The system creates a slot-type profile when it first detects the presence of a particular module. The system does not delete the profile unless you use the `slot -r` command to permanently remove a module that is no longer installed in the system, or clear nonvolatile RAM (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.

**Example** `set 72-ct-dmt-adsl = auto`

**Location** `LOAD-SELECT`

## 72-gs-dmt-adsl

**Description** Specifies whether code images for ADSL 72-port Globespan line interface modules (LIMs) are to be stored in flash memory.

**Usage** Valid values are as follows:

- **auto**—Causes the system to load images for ADSL 72-port Globespan LIMs that are installed in the Stinger unit and to skip images for modules that are not installed. This is the default.
- **load**—Causes the system to load the image, even if no ADSL 72-port Globespan LIMs are installed.
- **skip**—Causes the system to skip the image, even if an ADSL 72-port Globespan LIM is installed.



**Note** A module is considered present in the system if a slot-type profile exists for that module type. The system creates a slot-type profile when it first detects the presence of a particular module. The system does not delete the profile unless you use the `slot -r` command to permanently remove a module that is no longer installed in the system, or clear nonvolatile RAM (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.

**Example** `set 72-gs-dmt-adsl = auto`

**Location** `LOAD-SELECT`

#### 72-shdsl

**Description** Specifies whether code images for SHDSL 72-port line interface modules (LIMs) are to be stored in flash memory.

**Usage** Valid values are as follows:

- **auto**—Causes the system to load images for SHDSL 72-port LIMs that are installed in the Stinger unit and to skip images for modules that are not installed. This is the default.
- **load**—Causes the system to load the image, even if no SHDSL 72-port LIMs are installed.
- **skip**—Causes the system to skip the image, even if an SHDSL 72-port LIM is installed.



**Note** A module is considered present in the system if a slot-type profile exists for that module type. The system creates a slot-type profile when it first detects the presence of a particular module. The system does not delete the profile unless you use the `slot -r` command to permanently remove a module that is no longer installed in the system, or clear nonvolatile RAM (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.

**Example** `set 72-shdsl = auto`

**Location** `LOAD-SELECT`



## A

### aal5-encaps

**Description** Specifies the type of data encapsulation used over the ATM adaptation layer 5 (AAL5) service-specific convergence Sublayer (SSCS).

**Usage** Specify one of the following values:

- llc-encapsulation (the default)
- multi-frame-relay-sscs
- other-encapsulation
- vmux-bridged-8023
- vmux-bridged-8025
- vmux-bridged-8026
- vmux-lanemul-8023
- vmux-lanemul-8025
- vmux-routed:
- unknown-encapsulation

**Example** set aal5-encaps = vmux-bridged-8023

**Location** ATM-VCL-CONFIG

### aal-enabled

**Description** Enables ATM adaptation layer (AAL) options.

**Usage** Specify one of the following values:

- no—Disables AAL options. This is the default value.
- yes—Enables AAL options

**Example** set aal-enabled = yes

**Location** CONNECTION:atm-aal-options

### aal-type

**Description** The ATM adaptation layer (AAL) type.

**Usage** Set one of the following values:

- aal0—Sets AAL0 type of layer.
- aal5—Sets AAL5 type of layer.
- unspecified—Does not specify a type of AAL.

**Example** set aal-type = aal5

**Location** ATM-QOS

## *abstime*

**Description** Read-only. Indicates the absolute time, used as the index for error logging.

**Usage** Read-only value with the range 0 to 4294967295.

**Example** `abstime = 380038282`

**Location** `ERROR`

## *access-change-reason*

**Description** Reason for the change in this profile.

### **Permission level**

**Usage** Valid values are as follows:

- `unknown`—Unknown reason or the if the profile has not changed since it was created.
- `activation`—CLT access was activated.
- `deactivation`—CLT access was deactivated.
- `extension`—CLT duration was extended.
- `failure`—CLT access failed.

**Example** `access-change-reason = deactivation`

**Location** `CLT-MS-ACCESS-STAT`

## *access-end-date*

**Description** Specified end date of the test.

**Usage** A date in the format Day Month Year Date. The default setting for this parameter is Monday January 1990 1.

**Example** `access-end-date = { Monday January 1990 1 }`

**Dependencies** If you activate a test and do not specify a timeout value, the maximum system time is used, which is 23:59:59, 12/31/2089. This value changes accordingly when you extend test access.

**Location** `CLT-MS-ACCESS-STAT`

## access-end-time

**Description** Specified end time of the test.

**Usage** A time in the format HH:MM:SS. The default setting for this parameter is 0:0:0.

**Example** access-end-time = { 0 0 0 }

**Dependencies** If you activate a test and do not specify a timeout value, the maximum system time is used, which is 23:59:59, 12/31/2089. This value changes accordingly when you extend test access.

**Location** CLT-MS-ACCESS-STAT

## access-loop

**Description** Specifies the copper loop for a particular LIM port to be accessed in a copper loop test (CLT).

**Usage** Specify either 1 or 2. The default is 1.

**Example** set access-loop = 2

**Location** CLT-MS-ACCESS

## access-mode

**Description** Specifies the type of connection used in the configuration of the copper loop for a copper loop test (CLT).

**Usage** Valid values are as follows:

- bridged—Copper loop is connected to the test head and the corresponding port of the spare LIM.
- looking-out—Copper loop is connected only to the test head. This is the default.

**Example** set access-mode = looking-out

**Location** CLT-MS-ACCESS

## access-port

**Description** Specifies the port number of the copper loop to be tested.

**Usage** Enter the port number of the copper loop to be tested. The default is 1.

**Example** set access-port = 2

**Location** CLT-MS-ACCESS

## access-result

**Description** Indicates the current state of a copper loop test (CLT).

**Usage** Valid values are as follows:

- `idle`—Test head is inactive, and no copper loops are connected. This is the default
- `access-activated`—Test head is active, and a copper loop is connected as specified.
- `resource-busy`—Access failed. The resource to enable CLT module access is in use.

**Example** `set access-result = idle`

**Location** `CLT-MS-ACCESS`  
`CLT-MS-ACCESS-STAT`

## access-slot

**Description** Specifies the slot number of the line interface module (LIM) containing the copper loop to be tested.

**Usage** Enter the slot number, preceded by `slot-`, of the LIM. The default is `slot-16`.

Specify one of the following:

- `any-slot`—Special value used to specify any slot.
- `slot-1`—Slot 1.
- `slot-2`—Slot 2.
- `slot-3`—Slot 3.
- `slot-4`—Slot 4.
- `slot-5`—Slot 5.
- `slot-6`—Slot 6.
- `slot-7`—Slot 7.
- `slot-10`—Slot 10.
- `slot-11`—Slot 11.
- `slot-12`—Slot 12.
- `slot-13`—Slot 14.
- `slot-14`—Slot 14.
- `slot-15`—Slot 15.
- `slot-16`—Slot 16.

**Example** `set access-slot = slot-2`

**Location** `CLT-MS-ACCESS`

## access-start-date

**Description** Starting date of the test.

**Usage** A date in the format Day Month Year Date. The default setting for this parameter is Monday January 1990 1.

**Example** access-start-date = { Monday January 1990 1 }

**Location** CLT-MS-ACCESS-STAT

## access-start-time

**Description** Starting time of the test.

**Usage** A time in the format HH:MM:SS. The default setting for this parameter is 0:0:0.

**Example** access-start-time = { 0 0 0 }

**Location** CLT-MS-ACCESS-STAT

## access-terminal

**Description** Specifies the connection point of the copper loop used in the configuration of the copper loop for a copper loop test (CLT).

**Usage** Valid values are as follows:

- internal-tester-terminal—Copper loop is connected to the internal test head of the CLT module. This is the default.
- external-tester-terminal—Copper loop is connected to the external test terminals of the CLT module or path selector module (PSM).
- auxiliary-tester-terminal—Copper loop is connected to the auxiliary test terminals of the CLT module or PSM.
- external-loop—Internal test head of the CLT module is connected to external terminals.

**Example** set access-terminal = external-tester-terminal

**Location** CLT-MS-ACCESS

## access-timeout

**Description** Set a timeout value for a copper loop test.

**Usage** A value in minutes from 0 through 30.

**Example** set access-timeout = 5

**Location** CLT-MS-ACCESS

## acct-checkpoint

**Description** Specifies the interval (in seconds) at which to send checkpoint packets to the RADIUS daemon.

**Usage** Specify an integer from 0 to 60. The default is 0 (zero).

**Example** `set acct-checkpoint = 30`

**Location** `EXTERNAL-AUTH:rad-acct-client`

## acct-checkpoint-timer

**Description** Specifies whether to send RADIUS checkpoint accounting packets on a per-session basis.

**Usage** Specify one of the following settings:

- `per-session`—Specifies that checkpoint packets are sent on a per-session basis at the interval specified by the `acct-checkpoint` parameter.
- `all-sessions` (the default)—Specifies that checkpoint packets are all sent at the same time.

**Example** `set acct-checkpoint-timer = per-session`

**Dependencies** For `acct-checkpoint-timer` to apply, you must set `acct-type` to `radius`.

**Location** `EXTERNAL-AUTH:rad-acct-client`

## acct-drop-stop-on-auth-fail

**Description** Specifies whether RADIUS accounting stop packets are dropped for connections that fail authentication.

**Usage** Valid values are as follows:

- `yes`—Specifies that RADIUS Accounting Stop packets are dropped for connections that fail authentication.
- `no`—Specifies that RADIUS Accounting Stop packets are sent for connections that fail authentication. This is the default.

**Example** `set acct-drop-stop-on-auth-fail = yes`

**Location** `EXTERNAL-AUTH:rad-acct-client`

## acct-host

**Description** Specifies a RADIUS accounting server for the Stinger unit to use for the connection.

**Usage** Enter the IP address of a RADIUS accounting server. The default is 0.0.0.0, which causes the Stinger unit to look for an accounting server at the address specified by the `external-auth` profile.

**Example** `set acct-host = 10.9.8.2/24`

**Location** `CONNECTION:usrrad-options`

## acct-id-base

**Description** Specifies whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16. You can set `acct-id-base` globally and for each connection.

**Usage** Valid values are as follows:

- `acct-base-10`—Specifies a decimal base. This is the default.
- `acct-base-16`—Specifies a hexadecimal base.

The value you specify controls how the Stinger system presents the Acct-Session-ID attribute to the RADIUS accounting server.



**Note** The Acct-Session-ID attribute is defined in section 5.5 of the RADIUS accounting specification.

**Example** `set acct-id-base = acct-base-16`

**Dependencies** Consider the following:

- If `acct-type` does not specify `radius`, the `acct-id-base` value does not apply.
- Changing the value of `acct-id-base` while accounting sessions are active results in inconsistent reporting between the Start and Stop records.

**Location** `CONNECTION:usrrad-options`  
`EXTERNAL-AUTH:rad-acct-client`

## acct-key

**Description** Specifies a RADIUS shared secret. A shared secret acts as a password between the Stinger unit and the accounting server.

**Usage** Specify the text of the shared secret. The value you specify must match the value in the RADIUS `clients` file. If you specify a null value, the system logs the following warning:

warning: acct-key is empty (bad for security)

**Example** `set acct-key = mypw`

**Dependencies** If the `acct-type` parameter value does not specify `radius`, `acct-key` does not apply.

**Location** `CONNECTION:usrrad-options`  
`EXTERNAL-AUTH:rad-acct-client`

## acct-limit-retry

**Description** Specifies the maximum number of times the Stinger system tries to send accounting packets.

When the Stinger unit is configured for RADIUS accounting, it sends accounting Start and Stop packets to the RADIUS server to record connections. If the server does not acknowledge a packet within the number of seconds you specify for `acct-timeout`, the Stinger unit tries again, resending the packet until the server responds, or dropping the packet if the queue of packets to be resent is full. You can limit the number of retries by setting a maximum.

**Usage** To set the maximum number of retries for accounting packets, set `acct-limit-retry` to a value greater than 0 (zero). A value of 0 (the default) indicates an unlimited number of retries.



**Note** The Stinger unit always makes at least one attempt. For example, if you set the number of retries to 10, the Stinger unit makes 11 attempts—the original attempt plus 10 retries.

**Example** `set acct-limit-retry = 10`

**Location** `EXTERNAL-AUTH:rad-acct-client`

## acct-port

**Description** Specifies the UDP destination port to use for external accounting requests. When using RADIUS accounting, you can set `acct-port` globally and for each connection.

**Usage** Specify a UDP port number from 1 to 32767. The value must match the port number the accounting daemon uses. Following are the defaults for RADIUS:

- The default in a connection profile is 1646.
- The default in the `external-auth` profile is 0 (zero).

**Example** `set acct-port = 1500`

**Dependencies** If the `acct-type` parameter value does not specify `radius`, `acct-port` does not apply.

**Location** `CONNECTION:usrrad-options`  
`EXTERNAL-AUTH:rad-acct-client`



## acct-radius-compat

**Description** Enables or disables vendor-specific attribute (VSA) compatibility mode when the Stinger unit is using RADIUS for accounting purposes.

**Usage** Valid values are as follows:

- `old-ascend`—Specifies that the Stinger unit does not send the vendor-specific attribute to the RADIUS server and does not recognize the vendor-specific attribute if the server sends it. This is the default.
- `vendor-specific`—Specifies that the Stinger unit uses the vendor-specific attribute to encapsulate Lucent vendor attributes, and uses the RFC-defined User-Password encryption algorithm as well.

**Example** `set acct-radius-compat = vendor-specific`

**Location** `EXTERNAL-AUTH:rad-acct-client`

## acct-reset-time

**Description** Specifies the number of seconds that must elapse before the Stinger unit returns to using the primary RADIUS accounting server.

**Usage** Specify the number of seconds. The default is 0 (zero), which specifies that the Stinger unit does not return to using the primary RADIUS accounting server.

**Example** `set acct-reset-time = 60`

**Dependencies** For `acct-reset-time` to apply, you must specify at least one value for the `Acct-Server-N` parameter.

**Location** `EXTERNAL-AUTH:rad-acct-client`

## acct-server-n

**Description** Specifies the IP addresses of up to three external accounting servers. The Stinger unit first tries to connect to server 1. If it receives no response, it tries to connect to server 2. If it still receives no response, it tries to connect to server 3.

**Usage** Specify an IP address in dotted decimal notation. The default is 0.0.0.0, which indicates that no accounting server exists.

**Example** `set acct-server-1 = 10.2.3.4/24`

**Dependencies** Consider the following:

- If the `acct-type` parameter value does not specify `radius`, `acct-server-n` does not apply.
- If the Stinger unit connects to a server other than server 1, and `acct-reset-time` is set to 0, the Stinger unit continues to use that server until it fails to service requests, even if server 1 comes back online. If the `acct-reset-time` parameter is set to a value other than 0 (zero), the Stinger unit returns to using the primary accounting server after the number of seconds specified by `acct-reset-time` has elapsed.

**Location** `EXTERNAL-AUTH:rad-acct-client`

### acct-sess-interval

**Description** Specifies the number of seconds between RADIUS accounting reports that record the number of open sessions.

**Usage** Specify a number of seconds from 0 to 65535. The default is 0 (zero), which turns off regular RADIUS open-session reports.

**Example** `set acct-sess-interval = 15`

**Dependencies** If the `acct-type` parameter value does not specify RADIUS, `acct-sess-interval` does not apply. `Acct-Sess-Interval` has no effect unless the Lucent RADIUS daemon is running.

**Location** `EXTERNAL-AUTH:rad-acct-client`

### acct-src-port

**Description** Specifies the UDP source port to use for RADIUS accounting.

**Usage** Specify a value from 0 to 65535. The default is 0 (zero), which specifies that the Stinger unit selects the source port from the nonprivileged port range, 1024 through 2000.

**Example** `set acct-src-port = 3278`

**Dependencies** The Stinger unit uses the source port number to demultiplex the RADIUS reply packets to the appropriate line or trunk module. The system uses a separate source port for each module and shelf controller. On the Stinger unit, the actual source port is the value of `acct-src-port` plus the slot number. The slot number is 0 (zero) for the control module. So, if you set `acct-src-port` to 1000, packets originating from the control module have a source port value of 1000, while packets originating from slot 6 have a source port value of 1006.

**Location** `EXTERNAL-AUTH:rad-acct-client`

### acct-stop-only

**Description** Specifies whether the Stinger unit can send an Accounting Stop packet that does not contain a username. (At times, the Stinger unit can send an Accounting Stop packet to the RADIUS server without having sent an Accounting Start packet. These Stop packets have no username.)

**Usage** Valid values are as follows:

- `yes`—Specifies that the Stinger unit can send an Accounting Stop packet even if it does not contain a username. This is the default.
- `no`—Specifies that the Stinger unit cannot send an Accounting Sop packet if it does not contain a username.

**Example** `set acct-stop-only = no`

**Location** `EXTERNAL-AUTH:rad-acct-client`

## acct-timeout

**Description** Specifies the amount of time (in seconds) that the Stinger unit waits for a response to a RADIUS accounting request. You can set `acct-timeout` globally and for each connection.

If it does not receive a response within the specified time, the Stinger unit sends the accounting request to the next server specified by `acct-server-n`. If all RADIUS accounting servers are busy, the Stinger unit stores the accounting request and tries again at a later time. It can queue up to 154 requests.

**Usage** Specify an integer from 1 to 10. Following are the defaults:

- The default for a connection profile is 1.
- The default for the external-auth profile is 1.

**Example** `set acct-timeout = 5`

**Dependencies** If the `acct-type` parameter does not specify `radius`, `acct-timeout` does not apply.

**Location** CONNECTION:usrrad-options  
EXTERNAL-AUTH:rad-acct-client

## acct-tunnel-connection-encoding

**Description** Specifies an encoding method for the value of the RADIUS `Acct-Tunnel-Connection` attribute. NavisRadius™ software uses the value generated by the default setting of this parameter.

**Usage** Specify one of the following values:

- `normal`—Generates the `Acct-Tunnel-Connection` attribute value from the source and destination IP addresses, tunnel ID, and connection ID. This is the default.
- `decimal-call-serial-number`—Generates the `Acct-Tunnel-Connection` attribute value from the 32-bit Layer 2 Tunneling Protocol (L2TP) call serial number (CSN) encoded as a decimal string.
- `hexadecimal-call-serial-number`—Generates the `Acct-Tunnel-Connection` attribute value from the L2TP CSN encoded as a hexadecimal string.

**Example** `set acct-tunnel-connection = decimal-call-serial-number`

**Location** L2-TUNNEL-GLOBAL:l2tp-config

## acct-type

**Description** Specifies whether to use RADIUS accounting or no accounting at all. You can specify accounting globally and for each connection.

**Usage** To enable or disable accounting in the external-auth profile, specify one of the following values:

- `none`—Disables accounting. This is the default.
- `radius`—Enables RADIUS accounting.

To set accounting policy for a particular connection, specify one of the following values in the `connection` profile:

- `global`—Specifies that the Stinger unit sends accounting information to one of the accounting servers specified by the `external-auth` profile. This is the default.
- `local`—Specifies that the Stinger unit sends accounting information to the accounting server specified by `acct-host` in the `connection` profile.
- `both`—Specifies that the Stinger unit sends accounting information to both the global and local servers.

**Example** `set acct-type = radius`

**Dependencies** Consider the following:

- If you set `auth-type` to `radius/logout`, the Stinger unit disables RADIUS accounting. For `acct-type` to have any effect in a `connection` profile, you must set `auth-type` to `radius`.
- If you set `acct-type` to `radius`, you must set the `acct-server` parameter to specify at least one accounting server, and that server must be running a version of the daemon that specifically supports accounting.

**Location** `CONNECTION:usrrad-options`  
`EXTERNAL-AUTH`

### *accum-bit-err*

**Description** Read-only. Indicates the read-only number of actual bit errors detected during a continuous bit-error-rate test (BERT).

**Usage** The `accum-bit-err` value is read-only.

**Example** `accum-bit-err = 0`

**Location** `AL-DMT-STAT:physical-status`

### *acf-comp-enabled*

**Description** *Not used.* Specifies whether the PPP address and control field compression are enabled or disabled.

**Usage** Valid values are as follows:

- `yes`—Compression is enabled.
- `no`—Compression is disabled. This is the default.

**Location** `CONNECTION:ppp-options`

## action

**Description** Specifies an action to take on a route that matches the filter specification.

**Usage** Specify one of the following values:

- `add`—Increases the metric field of the matching routes by the `add-metric` value and then add them to the routing table.
- `accept`—Adds the matching routes to the routing table.
- `deny`—Rejects the matching routes (does not add them to the routing table).

**Example** `set action = add`

**Dependencies** This setting applies only if the `type` parameter in the `input filter` or `output filter` subprofile is set to `route-filter`.

**Location** `FILTER:input-filters[n]:route-filter`  
`FILTER:output-filters[n]:route-filter`

## activate-access

**Description** Indicates whether the copper loop is connected for a copper loop test (CLT).

**Usage** Valid values for this parameter are as follows:

- `yes`—Copper loop is connected as specified.
- `no`—Copper loop is disconnected from the test head or test terminals. This is the default.
- `extend`—Extend an active copper loop test beyond a specified timeout value. After you have written the profile, the setting of the `activate-access` parameter setting will be `yes`.

**Example** `set activate-access = extend`

**Location** `CLT-MS-ACCESS`

## activate-test

**Description** Activates or deactivates a test.

**Usage** Valid values are as follows:

- `yes`—Disconnects any existing calls on tested ports and begins the test.
- `no`—Reconnects any disconnected calls and stops the test. This is the default.

**Example** `set activate-test = yes`

**Location** `LINE-TESTS`

## activation

**Description** *Not currently used.*

**Usage** Leave the default value: static.

**Example** activation = static

**Location** AL-DMT:line-config

DS3-ATM:line-config

HDSL2:line-config

SHDSL:line-config

## active

**Description** Specifies the activation of an interface or feature. An active interface is available for use.

**Usage** Valid values are as follows:

In the mcast-service profile:

- yes—Service is enabled. Access to multicast groups by the client is controlled by this profile.
- no—Service is disabled. Access to any multicast groups by the client is blocked. This is the default value.

In the mcast-service:filter-list [n] profile:

- yes—Filter is enabled. Access to mcast-ip-address is controlled by filter-type parameter.
- no (the default)—Filter is disabled.

In other profiles:

- yes—Activates the interface or feature. This is the default in the debug, lim-sparing-status, switch-config, and vrouter profiles only.
- no—Makes the interface or feature unavailable for use. This is the default in all other profiles.

**Example** set active = yes

**Location** APS-CONFIG

CONNECTION

CONNECTION:ip-options:tos-options

DEBUG

FRAME-RELAY

IMA-GROUP

LIM-SPARING-CONFIG:auto-lim-sparing-config:lim-sparing-config [n]

LIM-SPARING-STATUS:lim-sparing-status [n]

MCAST-SERVICE

MCAST-SERVICE:filter-list [n]

MULTI-LINK-FR

IMAGROUP

IP-INTERFACE:ospf

PNNI-METRICS

PNNI-ROUTE-ADDR  
 PNNI-ROUTE-TNS  
 PNNI-SUMMARY-ADDR  
 SWITCH-CONFIG:atm-parameters:outgoing-queue:outgoing-queue [n]  
 VACM-ACCESS  
 VACM-SECURITY-GROUP  
 VACM-VIEW-TREE  
 VROUTER

## active-enabled

**Description** Specifies whether one of the following profiles is enabled or disabled:

- user profile—Specifies whether the profile is enabled or disabled. A disabled profile is not available for use. A dash appears before each inactive profile.
- snmpv3-notifications or snmpv3-target-param profile—Specifies whether the profile is used to generate notifications.
- trap profile—Specifies whether traps are sent to the host specified by the profile.

**Usage** Valid values are as follows:

In a user profile

- yes—Enables the user profile. This is the default.
- no—Disables the user profile.

In an snmpv3-notifications or snmpv3-target-param profile

- yes—Specifies that the profile is used to generate notifications.
- no—Specifies that the profile is not used to generate notifications. This is the default.

In a trap profile

- yes—Specifies traps are sent. This is the default.
- no—Specifies that traps are not sent.

**Example** set active-enabled = yes

**Location** USER

SNMPV3-NOTIFICATIONS

SNMPV3-TARGET-PARAM

TRAP

## activelinkcount

**Description** Read-only. Indicates the number of active data link connection identifiers (DLCI) in the permanent virtual circuit (PVC).

**Usage** Read-only numeric parameter with a range of 0 to 65535.

**Example** activelinkcount = 10

**Location** FRPVC-STAT

## active-route

**Description** Enables or disables the entry of a route in the routing table. (Setting the parameter to `no` is a useful way to make a route temporarily inactive, so you can reinstate the route later.)

**Usage** Specify `yes` or `no`. The default is `yes`, except for the `ip-route` profile called `default`. For the default `ip-route` profile, the default is `no`.

- `yes`—Activates the static route and add it to the routing table.
- `no`—Deactivates the route. An inactive route does not affect packet routing.

**Example** `set active-route = yes`

**Dependencies** The default route is an `ip-route` profile with the name `default` and a destination address of `0.0.0.0/0`. To activate the default route, you must set `gateway-address` to the IP address of the default router, and set `active-route` to `yes`.

**Location** `IP-ROUTE`

## active-upstream-bandwidth-on-trunks

**Description** Read-only. Indicates the active trunk-side bandwidth, based on the number of trunk ports and their status.

**Usage** The `active-upstream-bandwidth-on-trunks` value is read-only.

**Example** `active-upstream-bandwidth-on-trunks = 155540`

**Location** `BANDWIDTH-STATS`

## add-link-cond-time

**Description** *Not currently used.* Specifies the link conditioning time-out, in seconds, during link addition or insertion.

**Usage** Leave the default value.

**Example** `add-link-cond-time = 0`

**Location** `DS1-ATM:line-config:ima-option-config:txlink-config`  
`DS1-ATM:line-config:ima-option-config:rxlink-config`

## add-metric

**Description** Specifies a number to add to the metric value for a route that matches the route filter specification, if the specified value for the `action` parameter is `add`.

**Usage** Specify a number from 1 to 15. The number you specify must not result in a route metric greater than 15. The default is 0 (zero).

**Example** `set add-metric = 5`



**Dependencies** This setting applies only if in the input or output subprofile, the type parameter is set to route-filter and the action parameter is set to add.

**Location** FILTER:input-filters[n]:route-filter  
FILTER:output-filters[n]:route-filter

## add-persistence

**Description** Specifies the number of seconds that average line utilization (ALU) must persist beyond the target-utilization threshold before the Stinger unit adds bandwidth from available channels.

**Usage** Specify an integer from 1 to 300. The default is 5.

**Example** set add-persistence = 15

**Dependencies** Consider the following:

- When adding bandwidth, the unit adds the number of channels specified by increment-channel-count parameter in the mpp-options subprofile.
- When the seconds-history parameter value is high, add-persistence has little effect.

**Location** ANSWER-DEFAULTS:mpp-answer  
CONNECTION:mpp-options

## address

**Description** Specifies an address or a prefix to an address in one of several profiles. Depending on which profile the parameter is in, the address setting can be configurable or read-only.

**Usage** Address parameters have different uses in different profiles. The specific use of the address determines the number of bytes the address needs.

- In the atm-addr-alias profile, the address parameter specifies the Private Network-to-Network Interface (PNNI) node, the ATM end-system address, or a part of the end-system address. The number of bytes is specified in the length parameter setting in the same profile.
- In the addr-index subprofile of the pnni-route-addr profile, the address parameter specifies the prefix of a reachable ATM address.
- In the pnni-summary-addr profile, the address parameter specifies the prefix of a reachable ATM address.

**Example** set address = 47410017001700170017001700

**Location** ATM-ADDR-ALIAS  
ATM-IF-CONFIG  
ATM-IF-SIG-PARAMS  
ATM-IF-STAT  
PNNI-IF-CONFIG  
PNNI-SUMMARY-ADDR:addr-index

**See Also** address (ATM-PREFIX:pnni-node-prefix), address (ATM-PREFIX:spvc-address-prefix), address (ATM-PREFIX:svc-address-prefix)

`address (ATM-PREFIX:pnni-node-prefix)`

**Description** Specifies the address prefix for Private Network-to-Network Interface (PNNI) node ATM addresses.

**Usage** Enter an address prefix value from 1 to 13 bytes long. The default value is a prefix value generated from the primary controller serial number.

**Example** `set address = 39:84:0f:80:01:bc:72:00:01:bc:e7:6c:02`

**Dependencies** Whenever you explicitly configure an address or a prefix setting, the system uses the value you specify rather than the system-generated default. If you delete the atm-prefix profile, the system creates a new one at the next system startup.

**Location** ATM-PREFIX:pnni-node-prefix

**See Also** `address`, `address (ATM-PREFIX:spvc-address-prefix)`, `address (ATM-PREFIX:svc-address-prefix)`

`address (ATM-PREFIX:spvc-address-prefix)`

**Description** Specifies a prefix value used to generate the address in the default set of atm-spvc-addr-config profiles.

**Usage** Enter an address prefix value from 1 to 13 bytes long. The default value is 0.

**Example** `set address = 39:84:0f:80:01:bc:72:00:01:bc:e7:6c:02`

**Dependencies** With the default setting of 0, the value is taken from the `address` parameter in the `pnni-node-prefix` subprofile.

**Location** ATM-PREFIX:spvc-address-prefix

**See Also** `address (ATM-PREFIX:pnni-node-prefix)`, `address`, `address (ATM-PREFIX:svc-address-prefix)`

`address (ATM-PREFIX:svc-address-prefix)`

**Description** Specifies a prefix value used to generate the address in the default set of atm-svc-addr-config profiles.

**Usage** Enter an address prefix value from 1 to 13 bytes long. The default value is 0.

**Example** `set address = 39:84:0f:80:01:bc:72:00:01:bc:e7:6c:02`

**Dependencies** With the default setting of 0, the value is taken from the `address` parameter in the `pnni-node-prefix` subprofile.

**Location** ATM-PREFIX:svc-address-prefix

**See Also** `address (ATM-PREFIX:pnni-node-prefix)`, `address (ATM-PREFIX:spvc-address-prefix)`, `address`

## address-pool

**Description** Specifies a number of an address pool from which to acquire an address.

When pool chaining is enabled, a pool number within a chain includes addresses defined in all other pools within the chain. For example, if pools 1, 2, and 3 are in a pool chain, setting this parameter to 1 has the same effect as setting it to 2 or 3.

**Usage** Specify a number from 0 to 128. The default is 0 (zero).

**Example** `set address-pool = 5`

**Dependencies** If `address-pool` is set to 0 (zero) and `assign-address` is set to `yes`, the Stinger unit gets IP addresses from the first defined address pool.

**Location** CONNECTION:ip-options

advertize

**Description** Enables or disables an area border router's advertisement of an Open Shortest Path First (OSPF) area. Unadvertised areas allow certain networks to be intentionally hidden from other areas.

**Usage** Valid values are as follows:

- **yes**—The area border router summarizes and advertise routes from this area.
- **no (the default)**—The area border router does not summarize or propagate routes from this area.

**Example** set advertize = yes

**Location** OSPF-AREA-RANGE

## adv-node-id

**Description** Specifies the ID of a Private Network-to-Network Interface (PNNI) node that advertises reachability to the address prefix.

**Usage** You can enter the full 22-byte ID or an alias.

**Example** set adv-node-id =  
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0+

**Location** PNNI-ROUTE-ADDR

## adv-port-id

**Description** Specifies the identifier on the advertising node of the interface used to reach the address prefix.

**Usage** Specify a number from zero (0) to 2147483647. The default is 0.

**Example** set adv-port-id = 0

**Location** PNNI-ROUTE-ADDR

## agent-mode

**Description** Specifies whether the Stinger unit operates as an Ascend Tunnel Management Protocol (ATMP) Foreign Agent or Home Agent, or selects which of those two modes to use for different traffic streams.

**Usage** Specify one of the following values:

- tunnel-disabled (the default)—Disables ATMP.
- home-agent—Operates as a Home Agent.
- foreign-agent—Operates as a Foreign Agent.
- home-and-foreign-agent—Operates as both a Home Agent and a Foreign Agent.

**Example** `set agent-mode = foreign-agent`

**Dependencies** If you change the `agent-mode` setting from its default, the new value does not take effect until you reset the system.

**Location** ATMP

## agent-type

**Description** In an Ascend Tunnel Management Protocol (ATMP) Home Agent configuration, this parameter specifies `gateway-home-agent` (the default) or `router-home-agent`, depending on how the Home Agent accesses the home network.

**Usage** Specify one of the following values:

- gateway-home-agent (the default)—Delivers tunneled data to the home network without routing. The connection between the Home Agent and the home network must be a leased connection.
- router-home-agent—Routes tunneled data to the home network.

**Example** `set agent-type = router-home-agent`

**Dependencies** This setting applies only when the `agent-mode` parameter is set to `home-agent`.

**Location** ATMP

## aggregate

**Description** Specifies whether virtual circuits using this traffic shaper are to be aggregated or not.

**Usage** Valid values are as follows:

- yes—Virtual circuits are aggregated. If the parameter set to `yes` and the traffic shaper is applied to more than one virtual circuit, the combined virtual circuits share the full bandwidth defined in the shaper.
- no (the default)—Virtual circuits are not aggregated.

**Example** `set aggregate = yes`

**Location** `SYSTEM:traffic-shapers n`  
`ATM-INTERNAL:traffic-shapers n`

## aim-enabled

**Description** Read-only. Indicates whether the unit enables Ascend Inverse Multiplexing (AIM).

**Usage** The aim-enabled setting is read-only. Values are as follows:

- **yes**—Indicates that AIM is enabled.
- **no**—Indicates that AIM is not enabled. This is the default.

**Example** aim-enabled = yes

**Location** BASE

## ais-receive

**Description** Read-only. Indicates whether the remote end is sending an Alarm Indication signal (AIS) on the line. The remote end sends an AIS (instead of normal data) to take the line out of service.

**Usage** The ais-receive setting is read-only. Values are as follows:

- **true**—Indicates that the remote end is sending an AIS.
- **false**—Indicates that the remote end is not sending an AIS.

**Example** ais-receive = true

**Location** DS1-ATM-STAT  
DS3-ATM-STAT  
E3-ATM-STAT  
OC3-ATM-STAT  
T1-STAT

## alarm-clear-table-limit

**Description** Specifies the maximum number of alarms that can be stored in alarmClearTable.

**Usage** Specify a number from 1 through 200. The default is 100.

**Example** set alarm-clear-table-limit = 150

**Location** SNMP

## alarm-enabled

**Description** Specifies whether the Stinger unit traps alarm events and sends a trap protocol data unit (PDU) to the SNMP manager. The Ascend Enterprise MIB defines the following alarm events. For a complete list, see the *Stinger Administration Guide* or the Ascend Enterprise MIB.

**Alarm event**

coldStart  
(RFC-1215 trap-type 0)

warmStart  
(RFC-1215 trap-type 1)

linkDown  
(RFC-1215 trap-type 2)

linkUp  
(RFC-1215 trap-type 3)

frDLCIStatusChange  
(RFC-1315 trap-type 1)

eventTableOverwrite  
(Lucent trap-type 16)

**Indicates that the unit**

Is reinitializing itself in such a way that it might alter the configuration of either the SNMP manager or the unit.

Is reinitializing itself so that neither the configuration of the SNMP manager nor that of the unit will change.

Recognizes a failure in one of the communication links represented in the SNMP manager's configuration.

Recognizes that one of the communication links represented in the SNMP manager's configuration has come up.

Recognizes that one of the virtual circuits has changed states. The link has been created, invalidated, or toggled between the active and inactive states.

Detected that a new event has overwritten an unread event. Once sent, additional overwrites will not cause another trap to be sent until at least one table's worth of new events has occurred.

**Usage** Valid values are as follows:

- yes (the default)—Specifies that the Stinger unit sends alarm-event traps to the host specified in the host-address parameter setting in the TRAP profile.
- no—Specifies that the Stinger unit does not send alarm-event traps.

**Example** set alarm-enabled = no

**Location** TRAP

## alarm-led-major

**Description** Specifies the behavior of the MAJOR alarm status light when the system detects a major alarm.

**Usage** Valid values are as follows:

- `on`—The major alarm status light illuminates when the system detects the event specified by event in the alarm profile.
- `off` (the default)—The major alarm status light remains off when the system detects an event.

**Example** `set alarm-led-major = on`

**Location** `ALARM:action`

## alarm-led-minor

**Description** Specifies the behavior of the MINOR alarm status light when the system detects a minor alarm.

**Usage** Valid values are as follows:

- `on`—The minor alarm status light illuminates when the system detects the event specified by event in the alarm profile.
- `off` (the default)—The minor alarm status light remains off when the system detects an event.

**Example** `set alarm-led-minor = on`

**Location** `ALARM:action`

## alarm-relay-major

**Description** Specifies the behavior of the major alarm relay.

**Usage** Valid values are as follows:

- `on`—Sets the relay for the major alarm circuit to close when the system detects the condition specified by event.
- `off` (the default)—Sets the relay for the major alarm circuit to ignore the condition specified by event.

**Example** `set alarm-relay-major = on`

**Location** `ALARM:action`

## alarm-relay-major-duration

**Description** Specifies the number of seconds that the Stinger unit leaves alarm-relay-major in the position specified in the alarm-relay-major parameter.

**Usage** Specify an integer. The default is 0 (zero), which directs the Stinger unit to leave the alarm set indefinitely.

**Example** set alarm-relay-major-duration = 30

**Location** ALARM:action

## alarm-relay-minor

**Description** Specifies the behavior of the minor alarm relay.

**Usage** Valid values are as follows:

- on—Sets the relay for the minor alarm circuit to close when the system detects the condition specified by event.
- off (the default)—Sets the relay for the minor alarm circuit to ignore the condition specified by event.

**Example** set alarm-relay-minor = on

**Location** ALARM:action

## alarm-relay-minor-duration

**Description** Specifies the number of seconds that the Stinger unit leaves alarm-relay-minor in the position specified in the alarm-relay-minor parameter.

**Usage** Specify a number. The default is 0 (zero), which directs the Stinger unit to leave the alarm set indefinitely.

**Example** set alarm-relay-minor-duration = 30

**Location** ALARM:action

## alarm-state

**Description** Read-only. Indicates the status of the alarm specified by alarm-id.

**Usage** Valid values are as follows:

- alarm-active—Indicates that the alarm is active and appropriate action has been taken (setting status lights or closing relays).
- alarm-acknowledged—Indicates that the alarm has been acknowledged by the user.

**Example** alarm-state = alarm-active



**Note** You can acknowledge the alarm by using the alarm -a command.

**Location** ALARM-STAT



## alcatel-us-413-boost

**Description** Provides an increase in upstream rate in T1.413 mode for 24 or 48-port Annex A line interface modules (LIMs) based on the Globespan chip set when connected to Alcatel customer premises equipment (CPE).



**Caution** This parameter is irrelevant for any other situation. Use it with extreme caution.

**Usage** Specify one of the following values:

- `new`—Use with firmware releases 3.6.7.0 or later.
- `old`—Use with firmware release earlier than 3.6.7.0.
- `unknown`—Lucent Technologies recommends that this value be used for all firmware releases. This is the default value.

**Example** `set alcatel-us-413-boost = old`

**Location** `AL-DMT:line-config`

## al-dmtadsl-atm

**Description** Controls whether code images for ADSL line interface modules (LIMs) are to be stored in flash memory.

**Usage** Valid values are as follows:

- `auto`—Loads the code image if there is a module installed of that type. This is the default.
- `load`—Loads the image when one is present in the tar file
- `skip`—Skips the code image when one is present in the tar file

**Example** `set al-dmtadsl-atm = auto`

**Location** `LOAD-SELECT`

## alias-name

**Description** Specifies a name to represent the address identified the `atm-addr-alias` profile. This parameter provides a more convenient way of accessing the ATM address.

**Usage** Specify a string of up to 20 characters. The default is null.

**Example** `set alias-name = node1alias`

**Location** `ATM-ADDR-ALIAS`

## allow-as-client-dns-info

**Description** Enables or disables an exit mechanism to local servers if the client Domain Name System (DNS) servers are not found. To isolate local network information, set this parameter to *false*.

When specified in a *vrouter* profile, this DNS setting is exclusive to the virtual router. If DNS settings are not specified in a *vrouter* profile, the virtual router uses the DNS settings defined in the *ip-global* profile

**Usage** Valid values are as follows:

- *true* (the default)—Makes the local DNS servers accessible to PPP connections if the client DNS servers are unavailable.
- *false*—Does not make local DNS servers accessible to PPP connections if the client DNS servers are unavailable.

**Example** `set allow-as-client-dns-info = false`

**Location** *IP-GLOBAL*

*VROUTER*

## allow-auth-config-rqsts

**Description** Specifies whether the unit allows external configuration requests in authentication processing.

**Usage** Valid values are as follows:

- *yes* (the default)—Specifies that the unit allows external configuration requests in authentication processing.
- *no*—Specifies that the unit does not allow external configuration requests in authentication processing.

**Example** `set allow-auth-config-rqsts = no`

**Location** *EXTERNAL-AUTH:rad-auth-client*

## allow-code

**Description** Specifies whether permission to upload code to the Stinger unit and use the following code-level commands is enabled or disabled:

- *format*—Prepares a flash card for use.
- *fsck*—Checks the file system on a flash card.

**Usage** Valid values are as follows:

- *yes*—Grants permission to upload code to the Stinger unit.
- *no* (the default)—Denies permission to upload code to the Stinger unit.

**Example** `set allow-code = yes`

**Location** *USER*

## allow-debug

**Description** Enables or disables user access to debug commands.

**Usage** Specify one of the following values:

- no—User cannot use debug commands. This is the default value.
- yes—User can use debug commands.

**Example** `set allow-debug = yes`

**Location** USER

## allow-diagnostic

**Description** Specifies permission to all commands with a permission level of diagnostic, including the following:

| Command       | Description                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------|
| clock-source  | Display clock-source statistics.                                                                       |
| debug         | Enable or disable diagnostic output.                                                                   |
| device        | Start or halt a device.                                                                                |
| ether-display | Display the contents of received Ethernet packets.                                                     |
| if-admin      | Administer an interface.                                                                               |
| open          | Start a session with a line interface or trunk module.                                                 |
| ping          | Ping the specified host.                                                                               |
| slot          | Administer a line interface or trunk module.                                                           |
| telnet        | Open a Telnet session.                                                                                 |
| traceroute    | Display route statistics.                                                                              |
| uptime        | Report how long the system has been operational and how long individual modules have been operational. |

**Usage** Valid values are as follows:

- yes—Grants permission to use diagnostic commands.
- no (the default)—Denies permission to use diagnostic commands.

**Example** `set allow-diagnostic = yes`

**Location** USER

## allow-guaranteed-up-stream-bandwidth

**Description** Specifies the guaranteed upstream bandwidth for a slot.

**Usage** Specify an integer in kilobits per second. The default is 42500Kbps for each line interface module (LIM), which distributes the sum of 599040Kbps across the 14 LIM slots. Typically, slots with a high requirement for real-time traffic need high guaranteed bandwidth.

**Example** `set allow-guaranteed-up-stream-bandwidth = 80000`

**Dependencies** Even when the system is heavily loaded or the network is congested, the slot should be able to send upstream traffic at the rate of the specified `allow-guaranteed-up-stream-bandwidth` value. The total of all guaranteed upstream bandwidth for all slots cannot exceed the maximum upstream capacity of the system.

**Location** `SLOT-STATIC-CONFIG`

## allow-max-up-stream-bandwidth

**Description** Specifies the maximum upstream bandwidth for the slot.

**Usage** Specify a value in kilobits per second (Kbps) from 0 to 155000 (OC3 speed). The default is 70,000Kbps for each line interface module (LIM), and 1000Kbps for each control module.

**Example** `set allow-max-up-stream-bandwidth = 80000`

**Dependencies** For some LIMs, the default `allow-max-up-stream-bandwidth` setting of 70Mbps is too low, which can cause a fully loaded LIM to drop upstream data cells.

For any LIM that supports upstream bandwidth greater than 70Mbps, you must modify the default setting for the `allow-max-up-stream-bandwidth` parameter to prevent the module from dropping data cells when it is fully loaded.



**Note** A 155Mb throughput on a LIM is not guaranteed traffic. If a LIM allows traffic up to that limit, the system makes a best-effort attempt to deliver it.

**Location** `SLOT-STATIC-CONFIG`

## allow-password

**Description** Specifies permission to view passwords.

**Usage** Valid values are as follows:

- `yes`—Grants permission to view passwords.
- `no` (the default)—Denies permission to view passwords.

**Example** `set allow-password = yes`

**Location** `USER`

## allow-system

**Description** Enables or disables permission to use all commands with a permission level of `system`, including the following:

| Command                    | Description                                                            |
|----------------------------|------------------------------------------------------------------------|
| <code>arpable</code>       | Display or modify the Stinger address resolution protocol (ARP) table. |
| <code>clr-history</code>   | Clear the fatal-error history log.                                     |
| <code>connection</code>    | Display the connection-status window.                                  |
| <code>dir</code>           | List profiles and profile types.                                       |
| <code>dircode</code>       | Show the contents of the PCMCIA module code.                           |
| <code>fatal-history</code> | List the fatal-error history log.                                      |
| <code>get</code>           | Display settings in a profile.                                         |
| <code>iproute</code>       | Add or delete IP routes.                                               |
| <code>line</code>          | Display the line-status window.                                        |
| <code>list</code>          | List settings in the working profile.                                  |
| <code>log</code>           | Display and control the event-log window.                              |
| <code>netstat</code>       | Display the routing or interface tables.                               |
| <code>new</code>           | Create a new profile.                                                  |
| <code>read</code>          | Make the specified profile the working profile.                        |
| <code>refresh</code>       | Refresh the remote configuration.                                      |
| <code>set</code>           | Specify a value.                                                       |
| <code>show</code>          | Show shelves, slots, ports, or items.                                  |
| <code>status</code>        | Display the system status or hide the status window.                   |
| <code>userstat</code>      | Display user session status.                                           |
| <code>version</code>       | Display software-version information.                                  |
| <code>view</code>          | Change the contents of a status window.                                |

**Usage** Valid values are as follows:

- `yes`—Grants permission to use system commands.
- `no`—Denies permission to use system commands. This is the default.

**Example** `set allow-system = yes`

**Location** `USER`

## allow-termserv

**Description** *Not used.* Enables or disables permission to use the terminal server and its commands.

**Usage** Valid values are as follows:

- **yes**—Grants permission to use the terminal server and its commands.
- **no**—Denies permission to use the terminal server and its commands. This is the default.

**Example** `set allow-termserv = yes`

**Location** `USER`

## allow-unencrypted-tunnel-password

**Description** Enables or disables acceptance of unencrypted tunnel passwords from RADIUS.

**Usage** Specify one of the following values:

- **no** (the default)—Only encrypted tunnel passwords from RADIUS are accepted.
- **yes**—Unencrypted or encrypted tunnel-passwords are accepted from RADIUS.

**Example** `set allow-unencrypted-tunnel-password = yes`

**Dependencies** When this parameter is set to **yes**, RADIUS must encrypt the tunnel password before sending out to the tunnel server.

**Location** `EXTERNAL-AUTH:rad-auth-client`

## allow-update

**Description** Specifies permission to use all commands with a permission level of **update**, including the following:

| Command             | Description                                    |
|---------------------|------------------------------------------------|
| <code>date</code>   | Set the system date.                           |
| <code>delete</code> | Delete the specified profile.                  |
| <code>load</code>   | Load code or saved configuration to flash.     |
| <code>nvrw</code>   | Clear the configuration and reboot the system. |
| <code>reset</code>  | Reboot the system.                             |
| <code>save</code>   | Save a profile for a future restore.           |
| <code>write</code>  | Store the working profile and save changes.    |

**Usage** Valid values are as follows:

- **yes**—Grants permission to use update commands.
- **no**—Denies permission to use update commands. This is the default.

**Example** `set allow-update = yes`

**Location** `USER`

## `alpha-cell-delin-value`

**Description** Specifies the number of consecutive cells with incorrect header error control (HEC) that must be reached before the Stinger unit leaves the SYNC state (where the Stinger unit has correctly recognized cell boundaries) to go to the HUNT state (where the Stinger unit is still searching for the cell boundary) in an ATM connection.

**Usage** Specify a number from one to 16. The default is 7.

**Example** `alpha-cell-delin-value = 7`

**Location** `IMAHW-CONFIG`

## `alpha-ima-value`

**Description** Specifies the number of consecutive invalid IMA Control Protocol (ICP) cells that the Stinger unit must detect before changing to inverse multiplexing ATM (IMA) HUNT state (cell-by-cell validation) from the SYNC state (frame-by-frame validation).

**Usage** Specify the number 1 (one) or the number 2. The default is 2.

**Example** `set alpha-ima-value = 1`

**Location** `IMAHW-CONFIG`

## `annexb-anfp-enabled`

**Description** *Parameter for internal use only.*

**Location** `HDLSL2:line-config`  
`SHDSL:line-config`

**annexb-dmtadsl**

**Description** *Not used.* Specifies whether code images for 12-port Annex B ADSL line interface modules (LIMs) are to be stored in flash memory.

**Usage** Valid values are as follows:

- **auto**—Load the code image if there is a module installed of that type. This is the default.
- **load**—Load the code image when one is present in the tar file.
- **skip**—Skip the code image when one is present in the tar file.

**Example** `set annexb-dmtadsl = auto`

**Location** `LOAD-SELECT`

**ans-default**

**Description** *Not used.*

**Location** `CONNECTION:answer-options`

**ansi-adsl-ver**

**Description** Read-only. Indicates the supported issue of the ANSI T1.413 standard (issue 2).

**Usage** The `ansi-adsl-ver` value is read-only.

**Example** `ansi-adsl-ver = 2`

**Location** `AL-DMT-STAT:physical-status`

**answer-number-1**

**Description** Specifies the first telephone number to be used for the analog device attached to the Stinger unit. The Stinger unit uses this number, or the value in `answer-number-2`, to route all calls it receives with this number to the device.

**Usage** Enter a telephone number of up to 24 characters.

**Example** `set answer-number-1 = 747-5775`

**Location** `IDSL:line-interface`



## answer-number-2

**Description** Specifies a second telephone number to be used for the analog device attached to the Stinger unit. The Stinger unit uses this number, or the value in `answer-number-1`, to route all calls it receives with this number to the device.

**Usage** Enter a telephone number of up to 24 characters.

**Example** `set answer-number-2 = 747-5776`

**Location** `IDSL:line-interface`

## answer-originate

**Description** *Not supported.* Specifies whether the connection profile allows dial-out capability.

**Location** `CONNECTION:telco-options`

## apply-to

**Description** Specifies the direction in which type-of-service (TOS) settings are enabled.

**Usage** Specify one of the following values:

- `input` (the default)—Set bits in packets received on the interface.
- `output`—Set bits in packets transmitted on the interface.
- `both`—Set bits in packets sent and received on the interface.

**Example** `set apply-to = both`

**Dependencies** For this setting to apply, TOS and IP routing must be enabled in the connection profile.

**Location** `CONNECTION:ip-options:tos-options`

## aps-cfg-creation-time

**Description** Read-only. A timestamp that indicates the amount of time that has elapsed since the creation of the `aps-config` profile in automatic protection switching (APS). The TAOS timestamp shows the number of ticks since December 1, 1990.

**Usage** The valid range for this read-only parameter is from 0 through 2147483647.

**Example** `aps-cfg-creation-time = 356537747`

**Location** `APS-STAT`

### aps-channel-low-direction

**Description** Read-only. Indicates the state of lockout of the working (LOW) direction in the automatic protection (APS) system.

**Usage** Valid values for this read-only parameter are as follows

- low-none (the default)—No lock out of the working channel in either direction currently exists.
- low-recv—There is a lock out of the working channel in the receive direction.
- low-send—There is a lock out of the working channel in the send direction.
- low-both—There is a lock out of the working channel in the both directions.

**Example** `aps-channel-low-direction = none`

**Location** OC3-ATM-STAT

### aps-channel-recv-ais-count

**Description** Read-only. Indicates the count of Alarm Indication signal (AIS)-L errors received on the channel.

**Usage** The valid range for this read-only parameter is from 0 through 2147483647. The default is 0.

**Example** `aps-channel-recv-ais-count = 0`

**Location** OC3-ATM-STAT

### aps-channel-recv-rdi-count

**Description** Read-only. Indicates the count of restricted digital information (RDI)-L received on the protection channel.

**Usage** The valid range for this read-only parameter is from 0 through 2147483647. The default is 0.

**Example** `aps-channel-recv-rdi-count = 2`

**Location** OC3-ATM-STAT

### aps-channel-recv-sd-count

**Description** Read-only. Indicates the number of signal degrade conditions (line bit-error rates beyond the configured threshold) received over the K1K2 automatic protection switching (APS) channel from the far-end.

**Usage** The valid range for this read-only parameter is from 0 through 2147483647. The default is 0.

**Example** `aps-channel-rec-sf-condition = 0`

**Location** OC3-ATM-STAT

### aps-channel-recv-sf-condition

**Description** Read-only. Indicates the number of signal degrade conditions (line bit-error rates beyond the configured threshold) received over the K1K2 APS channel from the far-end.

**Usage** The valid range for this read-only parameter is from 0 through 2147483647. The default is 0.

**Example** `aps-channel-rec-sf-condition = 0`

**Location** OC3-ATM-STAT

### aps-channel-recv-sf-count

**Description** Read-only. Indicates the count of signal failure condition—loss of signal, loss of frame, Alarm Indication signal (AIS)-L or bit-error rate (BER) exceeding the configured threshold— received on the channel.

**Usage** The valid range for this read-only parameter is from 0 through 2147483647. The default is 0.

**Example** `aps-channel-rec-sf-condition = 0`

**Location** OC3-ATM-STAT

### aps-channel-sd-condition

**Description** Read-only. Indicates whether there is currently a signal degrade condition—line bit-error rates beyond the configured threshold—received over the K1K2 APS channel from the far end.

**Usage** Values for this read-only parameter are true and false.

**Example** `aps-channel-sd-condition = false`

**Location** OC3-ATM-STAT

### aps-channel-sf-condition

**Description** Read-only. Indicates whether there is currently a signal-failure condition—loss of signal, loss of frame, Alarm Indication signal (AIS)-L or bit-error rate (BER)— exceeding the configured threshold.

**Usage** The values for this read-only parameter are true and false.

**Example** `aps-channel-sf-condition = false`

**Location** OC3-ATM-STAT

### aps-channel-status

**Description** Read-only. Indicates the current status of the channel (port).

**Usage** Valid values for this read-only parameter are as follows:

- on-protection—The channel is currently switched to the protection channel.
- on-working—The channel is currently switched to the working channel.

**Example** `aps-channel-status = on-working`

**Location** OC3-ATM-STAT

### aps-config-name

**Description** Does one of the following:

- In the OC3-ATM profile, configures the protection group in a channel using automatic protection switching (APS).

The protection group is created for each OC3-ATM trunk port on the trunk aggregation module (TRAM) when the `aps-config` profile is configured and activated, and is referred to from one of the OC3-ATM profiles.

- In the OC3-ATM-STAT profile, indicates the name of the APS group.

**Usage** Specify the name of the `aps-config` profile.

**Example** `set aps-config-name = pg1`

**Location** OC3-ATM

OC3-ATM-STAT

### aps-enabled

**Description** Read-only. Indicates the license status of the automatic protection switching (APS) feature.

**Usage** Read-only parameter with the following values:

- no—APS feature is not enabled.
- yes—APS feature is enabled.

**Example** `aps-enabled = yes`

**Location** BASE

## aps-state

**Description** Indicates the current state of the protection group.

**Usage** Values for this read-only parameter are as follows:

- unknown— The state of protection group is unknown. Occurs when, for example, protection group is not started.
- on-protection— The active channel is currently the protection channel.
- on-working— The active channel is currently the working channel.

**Example** `aps-state = on-working`

**Location** APS-STAT

## area

**Description** Specifies the Open Shortest Path First (OSPF) area that the connection or interface belongs to.

**Usage** Specify an area ID in dotted decimal notation. The default is 0.0.0.0, which represents the backbone network.

**Example** `set area = 0.0.0.1`

**Location** CONNECTION:ip-options:ospf-options  
IP-INTERFACE:ospf

## area-id

**Description** Specifies the Open Shortest Path First (OSPF) area ID for this area range.

**Usage** Specify an area ID in dotted decimal notation. Area numbers are not IP addresses, although they use a similar format. The area ID of 0.0.0.0 is reserved for the backbone.

**Example** `set area-id = 0.0.0.2`

**Location** OSPF-AREA-RANGE

## area-network-addr

**Description** Specifies a network address range belonging to an area within an Open Shortest Path First (OSPF) autonomous system (AS). Network addresses with the same area id belong to the same OSPF area.

**Usage** Specify an IP address in dotted decimal notation. If the area represents a network subnet, enter the IP network number of the network subnet.

**Example** `set area-network-addr = 192.168.200.0`

**Location** OSPF-AREA-RANGE

## area-network-mask

**Description** Specifies the subnet mask for a network address range belonging to an area within an Open Shortest Path First (OSPF) autonomous system (AS).

**Usage** Specify a subnet mask in dotted decimal notation.

**Example** `set area-network-mask = 255.255.255.0`

**Location** `OSPF-AREA-RANGE`

## area-type

**Description** Specifies the type of Open Shortest Path First (OSPF) area that the connection or interface belongs to.

**Usage** Specify one of the following settings:

- `normal` (the default)—The router maintains information about external routes.
- `stub`—All external routes are summarized by a default route. A stub area is similar to a regular area, except that the routers do not enter external routes in the area's databases. For an area that has only one exit point, you need not maintain information about external routes.
- `nssa`—An OSPF not-so-stubby area (NSSA).

**Example** `set area-type = normal`

**Dependencies** You must set `area-type` consistently on all OSPF routers within the area. If you change the OSPF `area-type` from `normal` to `nssa` or vice versa, you must reset the system for the change to take effect.

**Location** `CONNECTION:ip-options:ospf-options`  
`IP-INTERFACE:ospf`

## as-boundary-router

**Description** Specifies whether the Stinger unit performs autonomous system border router (ASBR) calculations.

ASBRs perform calculations related to external routes. Normally, when the Stinger unit imports external routes from Routing Information Protocol (RIP), it performs the ASBR calculations for those routes. However, you can use the `as-boundary-router` setting to prevent the Stinger unit from performing ASBR calculations.

**Usage** Specify one of the following settings:

- `yes` (the default)—The Stinger unit performs ASBR calculations.
- `no`—The Stinger unit does not perform ASBR calculations.

**Example** `set as-boundary-router = no`

**Location** `IP-GLOBAL:ospf-global`

### ascend-adsl-trap-enabled

**Description** Enables or disables sending of the ADSL remote power-down trap (notification) and Ascend-specific ADSL link-down trap to the identified host.

**Usage** Select one of the following values:

- **yes**—Enables sending of the trap.
- **no**—Disables sending of the trap. This is the default value.

**Example** `set ascend-adsl-trap-enabled = yes`

**Location** TRAP

### ascend-cac-fail-trap-enabled

**Description** Enables or disables sending of a trap (notification) whenever a connection admission control (CAC) failure occurs for an Asynchronous Transfer Mode (ATM) connection.

**Usage** Select one of the following values:

- **yes**—Enables sending of the trap.
- **no**—Disables sending of the trap. This is the default value.

**Example** `set ascend-cac-fail-trap-enabled = yes`

**Location** TRAP

### ascend-enabled

**Description** Specifies whether the Stinger SNMP agent generates a trap (notification) to indicate a change of state in a host interface. All port connections are monitored by the system and reported by means of this trap.

**Usage** Valid values are as follows:

- **yes**—Specifies that a trap is generated to indicate a change of state in a host interface. This is the default.
- **no**—Specifies that a trap is not generated to indicate a change of state in a host interface.

**Example** `set ascend-enabled = no`

**Dependencies** If you set `ascend-enabled` to `yes`, you must also set `port-enabled` in the trap profile to `yes`.

**Location** TRAP

## ascend-flash-card-trap-enabled

**Description** Enables/disables the Stinger unit from generating a trap whenever you insert or remove a flash card from a control module.

**Usage** Valid values are as follows:

- yes (the default)—Enables trap generation.
- no—Disables trap generation.

**Example** `set ascend-flash-card-trap-enabled = no`

**Location** TRAP

## ascend-hashcode-mismatch-trap-enabled

**Description** Enables/disables the sending of a trap if the primary and secondary control modules have different software licenses enabled. By default, the system does not send a trap when the primary and secondary control modules have different software licenses enabled (this parameter is set to no). Specify yes to enable the system to send a trap.



**Note** If ascend-hashcode-mismatch-trap-enabled is enabled, the system sends only a single trap for all instances of mismatched software licenses between the control modules.

**Usage** Valid values are as follows:

- yes—Enables trap generation.
- no (the default)—Disables trap generation.

**Example** `set ascend-hashcode-mismatch-trap-enabled = yes`

**Location** TRAP

## ascend-link-down-trap-enabled

**Description** Specifies whether the system sends the Ascend link-down trap (notification) to the identified host when a failure occurs in a communication link between the unit and the SNMP manager.

**Usage** Specify one of the following values:

- yes—The system sends the Ascend link-down trap to the host.
- no (the default)—The system does not send the Ascend link-down trap to the host.

**Example** `set ascend-link-down-trap-enabled = yes`

**Dependencies** The linkdown-enabled parameter must be set to yes for this trap to be enabled.

**Location** TRAP



## ascend-link-up-trap-enabled

**Description** Specifies whether the system sends the Ascend link-up trap (notification) to the identified host when the communication link between the unit and the SNMP manager is reestablished.

**Usage** Specify one of the following values:

- `yes`—The system sends the Ascend link-up trap to the host.
- `no` (the default)—The system does not send the Ascend link-up trap to the host.

**Example** `set ascend-link-uptrap-enabled = yes`

**Dependencies** The `linkup-enabled` parameter must be set to `yes` for this trap to be enabled.

**Location** TRAP

## ascend-sw-mismatch-trap-enabled

**Description** Enables/disables the sending of a trap if the primary and secondary control modules have different software versions. By default, the system does not send a trap when the primary and secondary control modules have different software versions (this parameter is set to `no`). Specify `yes` to enable the system to send a trap.

**Usage** Valid values are as follows:

- `yes`—Enables trap generation.
- `no` (the default)—Disables trap generation.

**Example** `set ascend-sw-mismatch-trap-enabled = yes`

**Location** TRAP

## ase-tag

**Description** Specifies the Open Shortest Path First (OSPF) autonomous system external (ASE) tag for the link. The tag is attached to each external route.

The `ase-tag` setting is not used by the OSPF protocol itself. Area border routers (ABRs) can use it to filter a record.

**Usage** Specify a 32-bit hexadecimal number. The default is `c0:00:00:00`.

**Example** `set ase-tag = c8000000`

```
CONNECTION:ip-options:ospf-options
IP-INTERFACE:ospf
IP-ROUTE
```

## ase-type

**Description** Specifies the Open Shortest Path First (OSPF) autonomous system external (ASE) type of the link state advertisement (LSA).

**Usage** Specify one of the following settings:

- Type-1 (the default)—Specifies a type 1 external metric. This metric is expressed in the same units as the link-state metric.
- Type-2—Specifies a type 2 external metric. This metric is considered larger than any link-state path. Using a type 2 external metric assumes that routing between autonomous systems is the major cost of routing a packet. A type 2 metric eliminates the need for conversion of external costs to internal link-state metrics.

**Example** `set ase-type = type-1`

**Location** CONNECTION:ip-options:ospf-options  
IP-INTERFACE:ospf  
IP-ROUTE

## assign-address

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

**Usage** Valid values are as follows:

- yes—Assigns dynamic IP addresses to incoming calls as required.
- no (the default)—Disables dynamic IP address assignment.

**Example** `set assign-address = yes`

**Dependencies** The unit must have at least one configured pool of IP addresses. You can configure the pool locally or in RADIUS.

**Location** ANSWER-DEFAULTS:ip-answer

## assign-count [n]

**Description** An array of 128 elements, each of which can specify the number of host addresses contained in one IP address pool. For each pool, a contiguous block of addresses must be available, starting with the address you specify by using the `pool-base-address` parameter. The addresses in a pool are available for dynamic assignment to callers.

When specified in a `vrouter` profile, address pools are exclusive to that virtual router. If address pools are not specified in a `vrouter` profile, the virtual router(s) can share the address pools defined in the `ip-global` profile.

**Usage** For each pool, specify a number from 0 through 65535. The default is 0 (zero).

**Example** `set assign-count 1 = 25`  
`set pool-base-address = 1.1.1.125`

**Location** IP-GLOBAL  
VROUTER

## assignment-id

**Description** In a Layer 2 Tunneling Protocol (L2TP) mobile-client profile, this parameter specifies an identification (name) assigned to tunnels to allow grouping sessions. The value has local significance only. It is not transmitted to the remote tunnel end point.

**Usage** Specify a name of up to 31 characters. The default is null.

**Example** `set assignment-id = xyzserver`

**Dependencies** This setting applies only when `tunneling-protocol` is set to `l2tp-protocol` and `profile-type` is set to `mobile-client`.

**Location** `CONNECTION:tunnel-options`

## assign-vpi-vci

**Description** Specifies whether the virtual path identifier and virtual channel identifier (VPI-VCI) of the signaling virtual channel connection (VCC) is assigned locally or by the remote peer.

**Usage** Valid values are as follows:

- `yes`—Specifies that the local stack assigns the VPI-VCI. This is the default.
- `no`—Specifies that the remote peer assigns the VPI-VCI

**Example** `set assign-vpi-vci = yes`

**Location** `ATM-IF-SIG-PARAMS [n] :q2931-options`

## async-analog-profile

**Description** Specifies the connection profile name for asynchronous framing and analog bearer dial-out request.

**Usage** Specify an alphanumeric text string of up to 31 characters. The default value is blank.

**Example** `set async-analog-profile = analog_name`

**Location** `TUNNEL-SERVER:dialout-options`

## async-control-char-map

**Description** Read-only. A 4-byte (32-bit) field that indicates which of the 32 control codes are not to be sent in the clear.

**Usage** Read-only parameter consisting of four pairs of hexadecimal digits.

**Example** `async-control-char-map = 12:34:56:78`

**Location** `CONNECTION:ppp-options`

## async-digital-profile

**Description** Specifies the connection profile name for asynchronous framing and digital bearer dial-out request.

**Usage** Specify an alphanumeric text string of up to 31 characters. The default value is blank.

**Example** `set async-analog-profile = analog_name`

**Location** TUNNEL-SERVER:dialout-options

## at-answer-string

**Description** *Not used.*

## atm1483type

**Description** Specifies the multiplexing method for carrying multiple protocols over Asynchronous Transfer Mode (ATM) circuits by means of the ATM adaptation layer 5 (AAL5). Stinger systems support the encapsulation methods for carrying routed PDUs in the payload field of ATM adaptation layer (AAL) type 5 defined in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*.

**Usage** Valid values are as follows:

- `aal5-llc`—Specifies that system identifies the protocols by prefixing the protocol data unit (PDU) with an IEEE 802.2 Logical Link Control (LLC) header. This setting is used for non-PPP terminated connections such as RFC 2684 PVCs that terminate in the system. This is the default.
- `aal5-vc`—Specifies that the system performs higher-layer protocol multiplexing by creating separate ATM virtual circuits (virtual circuit multiplexing).

**Example** `set atm1483type = aal5-vc`

**Location** CONNECTION:atm-options  
CONNECTION:atm-connect-options

## atm-circuit-profile

**Description** Specifies the name of a connection profile that defines an Asynchronous Transfer Mode (ATM) circuit between a WAN interface and an ATM internal interface. These ATM circuits are used to switch incoming traffic directly from a WAN interface to a module that can process the data stream, such as a router module to route an IP data stream.

**Usage** Specify the name of a connection profile. The default value is an empty string.



**Caution** Currently, only ISDN digital subscriber line (IDSL) and router modules support ATM internal interfaces. This parameter has meaning in the `atm-options` subprofile only. Although it also appears in the `atm-connect-options` subprofile, the parameter is not used and must be left at the default null value.

**Example** `set atm-circuit-profile = ckt-7`

**Location** CONNECTION:atm-options  
CONNECTION:atm-connect-options

## atm-direct-enabled

**Description** Specifies whether the ATM direct feature is enabled.

**Usage** Specify one of the following settings:

- `yes`—Specifies that ATM direct is enabled.
- `no`—Specifies that ATM direct is disabled. This is the default value.

**Example** `set atm-direct-enabled = yes`

**Location** CONNECTION:atm-options

## atm-direct-profile

**Description** Specifies the name of the ATM connection profile to be used for the Asynchronous Transfer Mode (ATM) direct connection.

**Usage** Specify a name of up to 31 characters

**Example** `set atm-direct-profile = atmdirect`

**Location** CONNECTION:atm-options  
CONNECTION:atm-connect-options

## atm-enabled

**Description** Specifies whether Asynchronous Transfer Mode (ATM) is enabled for the connection.

**Usage** Valid values are as follows:

- `yes`—Specifies that ATM is enabled for the connection. This is the default.
- `no`—Specifies that ATM is not enabled for the connection.

**Example** `set atm-enabled = no`

**Dependencies** If the `encapsulation-protocol` parameter in the connection profile is not set to `atm` or `atm-circuit`, the value specified by `atm-enabled` does not apply.

**Location** CONNECTION:atm-options  
CONNECTION:atm-connect-options

**atm-if-delay**

**Description** Specifies the minimum time in seconds for IMA data cell rate (IDCR) changes between the subsequent ATM layer. This parameter pertains to inverse multiplexing ATM (IMA).

**Usage** The valid range is from 0 (zero) through 2147483647. The default is 0.

**Example** `set atm-if-delay = 0`

**Location** IMAGROUP

**atm-ima-alarm-trap-enabled**

**Description** Specifies whether the system sends the inverse multiplexing ATM (IMA) alarm trap (notification) to the identified host.

**Usage** Specify one of the following values:

- `yes`—The system sends the IMA alarm trap to the host.
- `no` (the default)—The system does not send IMA alarm trap to the host.

**Example** `set atm-ima-alarm-trap-enabled = yes`

**Location** TRAP

**atmp-enabled**

**Description** Indicates the license status for Ascend Tunneling Management Protocol (ATMP) tunnel protocol.

**Usage** Read-only parameter with possible values as follows:

- `yes`—ATMP tunnel protocol is enabled.
- `no`—ATMP tunnel protocol is not enabled.

**Example** `atmp-enabled = yes`

**Location** BASE

**atmp-ha-rip**

**Description** In an Ascend Tunnel Management Protocol (ATMP) Home Agent gateway profile, this parameter enables or disables construction of mobile-client routes in RIP-v2 responses to the home router. When this feature is enabled, the Home Agent informs the home router about routes to its mobile clients and saves the home router from maintaining a static route for each ATMP mobile client.

This feature also provides the basis for a resilient configuration, in which a secondary Home Agent can take over for a primary Home Agent if the primary agent becomes unavailable.

**Usage** Valid values are as follows:

- `rip-off` (the default)—Does not construct routes to mobile clients by using RIP.
- `rip-send-v2`—Sends the home router RIP-v2 response packets specifying mobile-client routes. The routes specify a mobile-client IP address and subnet mask, with the next hop set to 0.0.0.0 and the metric set to 1.

**Example** `set atmp-ha-rip = rip-send-v2`

**Dependencies** Consider the following:

- This parameter does not apply unless `profile-type` is set to `gateway-profile`.
- The `ip-options rip` parameter must be set to `routing-off` so that the home router does not send RIP updates to the Home Agent, which does not inspect them. Otherwise, RIP updates are forwarded, incorrectly, to the mobile clients.

**Location** `CONNECTION:tunnel-options`

## atmp-sap-reply

**Description** *Not supported.* Enables or disables a Home Agent's ability to reply to an IPX Nearest Server query.

**Location** `ATMP`

## atmp-snmp-trap

**Description** Enables or disables the following SNMP traps for the Ascend Tunnel Management Protocol (ATMP):

- `atmpMaxTunnelExceeded` (27)—Generated when the number of tunnels to a home network exceeds the maximum value.
- `atmpAgentErrorSen` (28)—Generated when errors have occurred at the agent level or with tunnel creation and are sent to the peer agent.
- `atmpAgentErrorRecvTrap` (29)—Generated when errors are received from the peer agent.

**Usage** Specify `yes` or `no`. The default value is `no`.

- `yes`—Enables ATMP SNMP traps.
- `no`—Does not enable ATMP SNMP traps.

**Example** `set atmp-snmp-trap = yes`

**Location** `ATMP`

## atm-pvc-failure-trap-enabled

**Description** Specifies whether the system sends the permanent virtual circuit (PVC) or soft PVC (SPVC) failure trap (notification) to the identified host.

**Usage** Specify one of the following values:

- **yes**—The system sends the PVC or soft PVC failure trap to the host.
- **no** (the default)—The system does not send the PVC or soft PVC failure trap to the host.

**Example** `set atm-pvc-failure-trap-enabled = yes`

**Location** TRAP

## atm-qos-rate-unit

**Description** Specifies the cell rate mode accepted in atm-qos profiles.

**Usage** Valid values are as follows:

- **kbps** - The following atm-qos cell-rate parameters are user-writable:
  - `peak-rate-kbits-per-sec`
  - `sustainable-rate-kbits-per-sec`
  - `minimum-rate-kbits-per-sec`

The system internally derives corresponding CPS values from these settings, and ignores user settings expressed in CPS. This is the default value.

- **cps** - The following atm-qos cell-rate parameters are user writable:
  - `peak-cell-rate-cells-per-sec`
  - `sustainable-cell-rate-cells-per-sec`
  - `minimum-cell-rate-cells-per-sec`

The system internally derives corresponding Kbps values from these settings, and ignores user settings expressed in Kbps..

**Example** `set atm-qos-rate-unit = cps`

**Dependencies** Cell rate values (PCR, SCR, and MCR) are expressed in paired sets of parameters in atm-qos profiles. Each cell rate is expressed in kilobits per second (kbps) and a corresponding cells per second (cps) value. Only one of each pair of parameters is user-writable, depending on atm-qos-rate-unit setting.



**Note** A system reset is recommended after changing the value of this parameter.

**Location** SYSTEM



## atm-service-category

**Description** Specifies the Asynchronous Transfer Mode (ATM) service class for the quality of service (QoS) contract. Also referred to as ATM service category.

**Usage** Valid values are as follows:

- **cbr**—Specifies constant bit rate, a service class for connections that depend on precise clocking to ensure undistorted delivery of bits. This is the default.
- **vbr-rt**—Specifies variable bit rate-real time a service class that handles the packaging of special delay-sensitive applications (such as packet video) that require low cell-delay variation between endpoints.
- **vbr-nrt**—Specifies a service class that handles packaging for the transfer of long, bursty data streams over a pre-established ATM connection.
- **ubr**—Specifies unspecified bit rate, a service class that handles bursty LAN traffic, as well as data that accepts delays and cell loss. It is a best-effort service that does not specify bit rates or traffic values, and offers no QoS guarantees.

**Example** `set atm-service-category = ubr`

**Dependencies** If `encapsulation-protocol` is not set to `ATM` or `ATM-Circuit`, `atm-service-category` does not apply.

**Dependencies** If `traffic-descriptor-type` is set to `clp-notagging-mcr`, `atm-service-category` must be set to `vbr-nrt`. If it is set to any other value, the system rejects the profile and displays an error message.

**Location** `ATM-QOS`

## attenuation-down

**Description** Read-only. Indicates the current downstream attenuation in decibels. Use this parameter to check the decrease in power of the signal in the downstream communication.

**Usage** The `attenuation-down` value is read-only.

**Example** `attenuation-down = 6`

**Location** `AL-DMT-STAT:physical-statistic`

## attenuation-up

**Description** Read-only. Indicates the current upstream attenuation in decibels. Use this parameter to check the decrease in power of the signal in the upstream communication.

**Usage** The `attenuation-up` value is read-only.

**Example** `attenuation-up = 41`

**Location** `AL-DMT-STAT:physical-statistic`

**atuc-15min-ess**

**Description** Specifies the number of errored seconds encountered by a DSL interface within any given 15-minute data collection period before a Simple Network Management Protocol (SNMP) notification (trap) is sent

**Usage** One notification is sent per interval per interface. A value of zero (0) disables the notification. Enter a value from 0 through 900.

**Example** `set atuc-15min-ess = 10`

**Location** DSL-THRESHOLD

**atuc-15min-lofs**

**Description** Specifies the number of loss-of-frame seconds encountered by a DSL interface within any given 15-minute data collection period before a Simple Network Management Protocol (SNMP) notification (trap) is sent.

**Usage** One notification is sent per 15 minute interval per interface. A value of 0 disables the trap. Enter a value from 0 through 900.

**Example** `set atuc-15min-lofs = 10`

**Location** DSL-THRESHOLD

**atuc-15min-lols**

**Description** Specifies the number of loss-of-link seconds encountered by a DSL interface within any given 15-minute data collection period before a Simple Network Management Protocol (SNMP) notification (trap) is sent.

**Usage** One notification is sent per interval per interface. A value of 0 disables the notification. Enter a value from 0 through 900.

**Example** `set atuc-15min-lols = 20`

**Location** DSL-THRESHOLD

**atuc-15min-loss**

**Description** Specifies the number of loss-of-signal-seconds encountered by a DSL interface within any given 15-minute data collection period before a Simple Network Management Protocol (SNMP) notification (trap) is sent.

**Usage** One notification is sent per 15-minute interval per interface. A value of 0 disables the trap. Enter a value from 0 through 900.

**Example** `set atuc-15min-loss = 28`

**Location** DSL-THRESHOLD

## atuc-15min-lprs

**Description** Specifies the number of loss-of-power seconds encountered by a DSL interface within any given 15-minute data collection period before a Simple Network Management Protocol (SNMP) notification (trap) is sent

**Usage** One notification is sent per interval per interface. A value of 0 disables the notification. Enter a value from 0 through 900.

**Example** `set atuc-15min-lprs = 10`

**Location** DSL-THRESHOLD

## atuc-fast-rate-down

**Description** Specifies the amount of change in rate of a fast channel that must occur to cause a notification (trap) to be sent. A notification is produced when the value of `atuc-fast-rate-down` exceeds the value of an internal parameter based on the channel rate down.

**Usage** Enter a value from zero (0) through 2147483647. A value of 0 disables the trap.

**Example** `set atuc-fast-rate-down = 0`

**Location** DSL-THRESHOLD

## atuc-fast-rate-up

**Description** Specifies the amount of change in rate of a fast channel that must occur to cause a notification (trap) to be sent. A notification is produced when the value of `atuc-fast-rate-up` exceeds the value of an internal parameter based on the channel rate up.

**Usage** Enter a value from 0 through 2147483647. A value of 0 disables the trap.

**Example** `set atuc-fast-rate-up = 0`

**Location** DSL-THRESHOLD

## atuc-init-failure-trap

**Description** Enables/disables InitFailureTrap.

**Usage** Specify enable or disable.

**Example** `set atuc-init-failure-trap = disable`

**Location** DSL-THRESHOLD

**atuc-interleave-rate-up**

**Description** Specifies the amount of change in rate of an interleaved channel that must occur to cause a notification (trap) to be sent. A notification is produced when the value of `atuc-interleave-rate-up` exceeds the value of an internal parameter based on the channel rate up.

**Usage** Enter a value from zero (0) through 2147483647. A value of 0 disables the trap.

**Example** `set atuc-interleave-rate-up = 0`

**Location** DSL-THRESHOLD

**atuc-interleave-rate-down**

**Description** Specifies the amount of change in rate of an interleaved channel that must occur to cause a notification (trap) to be sent. A notification is produced when the value of `atuc-interleave-rate-down` exceeds the value of an internal parameter based on the channel rate down.

**Usage** Enter a value from zero (0) through 2147483647. A value of 0 disables the trap.

**Example** `set atuc-interleave-rate-down = 0`

**Location** DSL-THRESHOLD

**atu-r**

**Description** Read-only. Indicates the results of the ADSL transceiver unit-remote (ATU-R) test.

**Usage** Read-only parameter with the following values:

- `no`—ATU-R is not present.
- `yes`—ATU-R is present.

**Example** `atu-r = yes`

**Dependencies** This test is valid only for ADSL line interface modules (LIMs).

**Location** CLT-RESULT

**atur-15min-ess**

**Description** Specifies the number of errored seconds encountered by a remote ADSL interface within any given 15-minute data collection period before a Simple Network Management Protocol (SNMP) notification is sent.

**Usage** One notification is sent per interval per interface. A value of zero (0) disables the notification. Enter a value from 0 through 900.

**Example** `set atur-15min-ess = 10`

**Location** DSL-THRESHOLD

**atur-15min-lofs**

**Description** Specifies the number of loss-of-frame seconds encountered by a remote ADSL interface within any given 15-minute data collection period before a Simple Network Management Protocol (SNMP) notification is sent.

**Usage** One notification is sent per 15-minute interval per interface. A value of 0 disables the trap. Enter a value from 0 through 900.

**Example** `set atur-15min-lofs = 10`

**Location** DSL-THRESHOLD

**atur-15min-loss**

**Description** Specifies the number of loss-of-signal-seconds encountered by a remote ADSL interface within any given 15-minute data collection period before a Simple Network Management Protocol (SNMP) notification is sent.

**Usage** One notification is sent per 15-minute interval per interface. A value of 0 disables the trap. Enter a value from 0 through 900.

**Example** `set atur-15min-loss = 28`

**Location** DSL-THRESHOLD

**atur-15min-lprs**

**Description** Specifies the number of loss-of-power seconds encountered by a remote ADSL interface within any given 15-minute data collection period before a Simple Network Management Protocol (SNMP) notification is sent

**Usage** One notification is sent per interval per interface. A value of 0 disables the notification. Enter a value from 0 through 900.

**Example** `set atur-15min-lprs = 10`

**Location** DSL-THRESHOLD

**atur-fast-rate-down**

**Description** Specifies the decrease in rate of a fast channel that will cause a trap to be sent.

**Usage** Specify a value from 0 to 4294967295. A value of 0 disables the trap.

**Example** `set atuc-fast-rate-down = 0`

**Dependencies** This parameter applies to fast channels only.

**Location** DSL-THRESHOLD

**atur-fast-rate-up**

**Description** Specifies the increase in rate of a fast channel that will cause a trap to be sent.

**Usage** Specify a value from 0 to 4294967295. A value of 0 disables the trap.

**Example** `set atuc-fast-rate-up = 0`

**Dependencies** This threshold applies to fast channels only.

**Location** DSL-THRESHOLD

**atur-interleave-rate-down**

**Description** Specifies the decrease in rate of an interleaved channel that will cause a trap to be sent.

**Usage** Specify a value from 0 to 4294967295. A value of 0 disables the trap.

**Example** `set atur-interleave-rate-down = 0`

**Dependencies** This parameter applies to interleaved channels only.

**Location** DSL-THRESHOLD

**atur-interleave-rate-up**

**Description** Specifies the increase in rate of an interleaved channel that will cause a trap to be sent.

**Usage** Specify a value from 0 to 4294967295. A value of 0 disables the trap.

**Example** `set atur-interleave-rate-up = 0`

**Dependencies** This parameter applies to interleaved channels only.

**Location** DSL-THRESHOLD

## audit-user-profiles

**Description** Enables/disables system monitoring of user profiles for expired passwords or user accounts.

**Usage** Valid values are as follows:

- **yes**—Enables the system to audit user profiles for expired passwords and user accounts. If a user account is expired, the system disables that account and terminates any active user sessions. A user with an expired account is denied access to the system.
- **no** (the default)—Disables auditing of user profiles for expired passwords or user accounts.

**Example** `set audit-user-profiles = yes`

**Dependencies** If the `audit-user-profiles` parameter is set to `yes`, by default, a user account expires after three years and a password expires after 60 days.



**Note** The system-generated user profile `admin` and its password do not expire. Users with Admin privileges can modify user account and password expiration dates.

**Location** `SYSTEM`

## auth-attribute-type

**Description** Specifies the attribute(s) used for session matching.

**Usage** Valid values are as follows

- **rad-serv-attr-any**—Specifies that the first Remote Authentication Dial-In User Service (RADIUS) attribute is used for session matching. This is the default.
- **rad-serv-attr-key**—Specifies that the session key is used for session matching.
- **rad-serv-attr-all**—Specifies that all attributes must match for session matching.

**Example** `set auth-attribute-type = rad-serv-attr-any`

**Dependencies** If the `rad-serv-enable` parameter in the `external-auth` profile is set to `no`, `auth-attribute-type` does not apply.

**Location** `EXTERNAL-AUTH:rad-auth-server`

## auth-boot-host

**Description** Specifies the IP address of the authentication boot host.

**Usage** Specify the IP address in dotted decimal notation.

**Example** `set auth-boot-host = 10.2.3.4`

**Location** `EXTERNAL-AUTH:rad-auth-client`

## auth-boot-host-2



**Note** This setting is for a customer-specific application outside of the United States. It is not intended for general use.

**Description** Specifies the IP address of the secondary RADIUS server to which ZGR answer-number requests, subaddress requests, and external-configuration requests are sent. External-configuration requests include requests for banner configurations, IP address pools, frame relay link configurations, dial-out profiles, answer numbers, ZGR answer numbers, and dial-out routes.

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

**Example** `set auth-boot-host-2 = 200.54.6.79`

**Dependencies** For auth-boot-host-2 to apply, you must set auth-type to radius.

**Location** EXTERNAL-AUTH:rad-auth-client

## auth-boot-port

**Description** Specifies the user datagram protocol (UDP) port to use for RADIUS authentication.

**Usage** Specify a number between zero (0) and 65535.

**Example** `set auth-boot-port = 1111`

**Location** EXTERNAL-AUTH:rad-auth-client

## auth-client n

**Description** Specifies up to nine IP addresses of Remote Authentication Dial-In User Service (RADIUS) clients permitted to issue RADIUS commands for session termination and filter changes.

**Usage** Specify an IP address in dotted decimal notation. The address 255.255.255.255 indicates that any client can issue RADIUS commands. (Currently, a maximum of nine clients is supported.) The default is 0.0.0.0, which indicates that no client can issue RADIUS commands.

**Example** `set auth-client 1 = 10.2.3.4`

**Dependencies** If the rad-serv-enable parameter in the external-auth profile is set to no, auth-client n does not apply. In addition, if you do not use auth-netmask n to supply a subnet mask, the system supplies a default subnet mask based on the address class.

**Location** EXTERNAL-AUTH:rad-auth-server



## auth-cli-user-dnis

**Description** Specifies a pseudo-dialed number identification service (DNIS) number for Telnet command-line interface users that need to be authenticated by the RADIUS server.

Specifying a value for this parameter enables a unit to use the DNIS number as a proxy to send access requests to a RADIUS server that holds the Telnet user accounts.

**Usage** Specify an integer of up to 40 characters.

- If the value is not null, the number is sent to RADIUS in Access Request packets as the DNIS attribute Called-Station-Id.
- If the value of auth-cli-user-dnis is null, Called-Station-Id is not sent.

**Example** `set auth-cli-user-dnis = 5051`

**Dependencies** The auth-cli-user-dnis value applies only when the cli-user-auth parameter is not set to local-only.

**Location** EXTERNAL-AUTH:rad-auth-client

## authen-key

**Description** Specifies an authentication key that appears in Open Shortest Path First (OSPF) virtual link configurations. The value of authen-key is a 64-bit clear password inserted into the OSPF packet header. It is used between two OSPF virtual link routers for authenticating traffic in the router's area.

**Usage** Specify a string of up to eight characters.

**Example** `set authen-key = lucospf2`

**Dependencies** authen-key does not apply if authen-type is set to none.

**Location** OSPF-VIRTUAL-LINK

## authentication-enabled

**Description** Specifies whether the system generates a notification (trap) when an authentication failure occurs.

**Usage** Valid values are as follows:

- yes—Specifies that the system generates a trap when an authentication failure occurs. This is the default.
- no—Specifies that the system does not generate a trap when an authentication failure occurs.

**Example** `set authentication-enabled = no`

**Location** TRAP

## authen-type

**Description** Specifies the type of authentication to use for validating Open Shortest Path First (OSPF) packet exchanges.

**Usage** Specify one of the following settings:

- **none**—Specifies that routing exchanges are not authenticated. The 64-bit authentication field in the OSPF header can contain data, but it is not examined on packet reception. When you use this setting, the Stinger unit performs a checksum on the entire contents of each OSPF packet (other than the 64-bit authentication field) to ensure against data corruption.
- **simple**—Requires that you specify a 64-bit value for **auth-key**. Each packet sent on a particular network must have the configured value in its OSPF header's 64-bit authentication field. Simple authentication is designed to prevent configuration errors from affecting the OSPF routing database. It is not designed for firewall protection. This is the default.
- **md5**—Specifies that the Stinger unit validates OSPF packet exchanges by using MD5 encryption and an authentication key ID that you specify by means of the **key-id** setting. Packets must contain the specified value in the OSPF header Key ID field to be allowed into the router's OSPF area.

**Example** `set authen-type = md5`

**Location** CONNECTION:ip-options:ospf-options  
IP-INTERFACE:ospf  
OSPF-VIRTUAL-LINK

## auth-frm-adr-start

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

**Usage** Valid values are as follows:

- **yes**—Enables the Stinger unit to send a second RADIUS Accounting Start record when the RADIUS Framed-Address value is assigned.
- **no**—Prevents the Stinger unit from sending a second RADIUS Accounting Start record. This is the default.

**Example** `set auth-frm-adr-start = yes`

**Location** EXTERNAL-AUTH:rad-auth-client

## auth-id-fail-return-busy

**Description** Specifies whether the Stinger unit returns user `busy` (decimal 17) or normal call clearing (decimal 16) as the cause element in ISDN Disconnect packets when calling line ID (CLID) or called-number authentication fails.

**Usage** Specify one of the following settings:

- `yes`—Specifies that the Stinger unit returns user `busy` (decimal 17) when CLID or called-number authentication fails.
- `no`—Specifies that the Stinger unit returns normal call clearing (decimal 16) when CLID or called-number authentication fails. This is the default.

**Example** `set auth-id-fail-return-busy = yes`

**Dependencies** For `auth-id-fail-return-busy` to apply, you must set `auth-type` to `radius`.

**Location** `EXTERNAL-AUTH:rad-auth-client`

## auth-id-max-retry-time

**Description** Specifies the maximum time limit for retrying RADIUS servers during the process of ID authentication.

**Usage** Specify a number between zero (0) and 10. A value of 0 sets the limit to the internal default value.

**Example** `set auth-id-max-retry-time = 0`

**Location** `EXTERNAL-AUTH:rad-auth-client`

## auth-id-timeout-return-busy

**Description** Specifies whether the Stinger unit returns User Busy (decimal 17) or Normal Call Clearing (decimal 16) as the Cause Element in ISDN Disconnect packets when called line ID (CLID) or dialed number identification service (DNIS) times out.

**Usage** Valid values are as follows:

- `yes`—Specifies that the Stinger unit returns User Busy (decimal 17) when CLID or called-number authentication times out.
- `no`—Specifies that the Stinger unit returns Normal Call Clearing (decimal 16) when CLID or called-number authentication times out. This is the default.

**Example** `set auth-id-timeout-return-busy = yes`

**Location** `EXTERNAL-AUTH:rad-auth-client`

#### auth-keep-user-name

**Description** Specifies how to handle the RADIUS *User-Name* attribute.

**Usage** Valid values are as follows:

- *change-name*—Specifies that the name provided by the server is used for the status display and for RADIUS accounting purposes. This is the default.
- *keep-name*—Specifies that the Stinger unit does not use the username returned by the server. If a name has been specified—that is, if called line ID (CLID) or dialed number identification service (DNIS) authentication is not used—the system uses that name. Otherwise, the system uses the name sent to the server for authentication.
- *keep-realm-name*—Specifies that if the username sent to the server for authentication is in a *realm*, the system behaves as if *auth-keep-user-name* is set to *keep-name*. (For example, if the username contains one of the characters @, \, /, or %, the username is in a realm.) Otherwise, the system behaves as if *change-name* is specified.



**Note** A user authenticated by called line ID (CLID) or dialed number identification service (DNIS) will appear to have the CLID or DNIS number as his or her username. If this condition is a problem, set *auth-keep-user-name* to *keep-realm-name*.

**Example** `set auth-keep-user-name = keep-name`

**Location** `EXTERNAL-AUTH:rad-auth-client`

#### auth-key

**Description** Specifies an authentication key that appears in Open Shortest Path First (OSPF), SNMPv3 user-based security model (USM), and external authentication configurations:

- For OSPF, the value of *auth-key* is a 64-bit clear password inserted into the OSPF packet header. It is used by OSPF routers for authenticating traffic in the router's area.
- For SNMPv3 USM configurations, *auth-key* is an authentication key generated by the `snmpAuthPass` command.
- For RADIUS, the *auth-key* value is a string of up to 22 characters. Because the Stinger unit can act both as a client to external servers and as a server responding to client commands, you can set *auth-key* in both the `rad-auth-client` and `rad-auth-server` subprofiles.

**Usage** The value you specify depends upon your configuration:

- For OSPF, specify a string of up to nine characters. The default is `ascend0`.
- For RADIUS, specify up to 22 characters. The default is null. For security purposes, the string is hidden when `auth-key` is displayed. If you specify a null value, the system logs the following warning:  
`warning: auth-key is empty (bad for security)`
- For most SNMPv3 USM configurations, do not set the 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.

**Example** Suppose you use the `snmpAuthPass` command to generate the following 16-byte string for an SNMPv3 USM configuration:

```
27 0a dc 75 f8 98 e5 7c 4c 03 22 7d dd ac 0d ef
```

The system displays this value as the following `auth-key` value:

```
'\x0a\xdcu\xf8\x98\xe5|L\x03"}\xdd\xac\x0d\xef
```

**Dependencies** Consider the following:

- For OSPF routing, `auth-key` does not apply if `authen-type` is set to `none`.
- For `auth-key` to apply in a RADIUS configuration, you must set `auth-type` to `radius`.
- For SNMPv3 USM configurations, `auth-key` does not apply if `auth-protocol` is set to `no-auth`.
- You must generate the authentication key by means of the `snmpAuthPass` command before the `snmpv3-usm-user` profile can be used for communication with the SNMP manager.
- If you change the authentication protocol from message-digest algorithm 5 (MD5) to secure hash algorithm (SHA) (or vice versa) for an SNMPv3 USM configuration, you must change the authentication key by means of the `snmpAuthPass` command. The previous protocol-and-key combination is used until you specify a new one.
- If you change the value of `auth-key` directly for SNMPv3 USM, keep in mind that the length of the escape sequence must be 10 (16D in hexadecimal) if MD5 is in use and 14 (20D in hexadecimal) if SHA is in use. If you specify an invalid value, the unit uses the previous key, if one exists, to communicate with the SNMP manager. If no previous key exists, this USM user cannot communicate with the network until a valid key is set by means of the `snmpAuthPass` command.

**Location** CONNECTION:ip-options:ospf-options

EXTERNAL-AUTH:rad-auth-client

EXTERNAL-AUTH:rad-auth-server

IP-INTERFACE:ospf

SNMPV3-USM-USER

## auth-netmask n

**Description** Specifies up to nine subnet masks. The Stinger unit matches each mask to the IP addresses of a Remote Authentication Dial-In User Service (RADIUS) client permitted to issue RADIUS commands for session termination and filter changes.

**Usage** Specify a subnet mask in dotted decimal notation. The default is 0.0.0.0.

**Example** `set auth-netmask 1 = 255.255.255.248`

**Dependencies** If the `rad-serv-enable` parameter is set to `no`, or if no `auth-client n` setting specifies an IP address, `auth-netmask n` does not apply.

**Location** `EXTERNAL-AUTH:rad-auth-server`

## auth-pool

**Description** Enables or disables allocation of an IP address from the default pool.

**Usage** Select one of the following values:

- `yes`—Enables allocation of IP address from the pool. Address is passed to the RADIUS server.
- `no`—Disables allocation of IP addresses from the pool. This is the default.

**Example** `set auth-pool = yes`

**Location** `EXTERNAL-AUTH:rad-auth-client`

## auth-pool-add

**Description** Internal field, not settable from user interface.

**Usage** Read-only IP address or netmask field.

**Example** `auth-pool-add = 192.207.23.13`

**Location** `CONNECTION:ip-options`

## auth-port

**Description** Specifies the UDP port to use for communication with the external authentication server. The value you specify must match the port specified for use in the server's configuration.

**Usage** Specify the UDP destination port to use for authentication. The default UDP port used by the RADIUS daemon is specified in the `/etc/services` file (UNIX).

**Example** `set auth-port = 1565`

**Location** `EXTERNAL-AUTH:rad-auth-client`  
`EXTERNAL-AUTH:rad-auth-server`  
`EXTERNAL-AUTH:tac-auth-client`  
`EXTERNAL-AUTH:tacplus-auth-client`

## auth-protocol

**Description** Specifies authentication of messages sent on behalf of this user to or from the Simple Network Management Protocol (SNMP) engine and, if enabled, the type of authentication protocol to be used.

**Usage** Valid values are as follows:

- `no-auth`—Disables authentication for this user.
- `md5-auth`—Enables authentication and specifies that the message-digest algorithm 5 (MD5) must be used. This is the default.
- `sha-auth`—Enables authentication and specifies that the secure hash algorithm (SHA) must be used.

**Example** `auth-protocol = md5-auth`

**Dependencies** If this parameter is set to a value other than `no-auth`, the `password` parameter must specify the password to be used.

**Location** `SNMPV3-USM-USER`

## auth-radius-compat

**Description** Enables or disables vendor-specific attribute (VSA) compatibility mode when the Stinger unit is using RADIUS for authentication and authorization purposes.

**Usage** Valid values are as follows:

- `old-ascend`—The Stinger unit does not send the vendor-specific attribute to the RADIUS server and does not recognize the vendor-specific attribute if the server sends it. This is the default.
- `vendor-specific`—The Stinger unit uses the vendor-specific attribute to encapsulate Lucent vendor attributes, and uses the RFC-defined User-Password encryption algorithm as well.

**Example** `set auth-radius-compat = vendor-specific`

**Location** `EXTERNAL-AUTH:rad-auth-client`  
`EXTERNAL-AUTH:rad-auth-server`

## auth-realm-delimiters

**Description** Specifies the characters that delimit a realm from the username.

**Usage** Specify up to seven characters in any order. The default is `@\/%`. If you do not specify any characters, the system behaves as though `auth-keep-user-name` is set to `change-name`.

**Example** `set auth-realm-delimiters = "%"`

**Dependencies** The `auth-realm-delimiters` setting does not apply unless `auth-keep-user-name` is set to `keep-realm-name`.

**Location** `EXTERNAL-AUTH:rad-auth-client`

## auth-req-delim-count

**Description** Specifies the number of delimiters to strip from a username in a RADIUS authentication request.

**Usage** Specify a number between zero (0) and 65535. The default is 0.

**Example** `set auth-req-delim-count = 2`

**Dependencies** You must be sure that the delimiters to strip are specified in the `auth-realm-delimiters` parameter.

**Location** `EXTERNAL-AUTH:rad-auth-client`

## auth-req-strip-side

**Description** Specifies the side from which to strip characters in a username of a RADIUS authentication request.

**Usage** Valid values are as follows:

- `none` (the default)—Does not strip characters from a username.
- `left`—Strips characters from the left side of the username.
- `right`—Strips characters from the right side of the username.

**Example** `set auth-req-strip-side = left`

**Dependencies** The `auth-req-delim-count` value must be greater than zero (0) for this parameter to take effect.

**Location** `EXTERNAL-AUTH:rad-auth-client`

## auth-reset-time

**Description** Specifies the authentication-timeout period, in seconds, after which the Stinger unit returns to the primary RADIUS authentication server. (The `auth-server-n` setting specifies the primary RADIUS authentication server.)

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

**Example** `set auth-reset-time = 60`

**Dependencies** For `auth-reset-time` to apply, you must specify at least one value for `auth-server-n`.

**Location** `EXTERNAL-AUTH:rad-auth-client`



## auth-retries

**Description** Specifies the number of times the Stinger unit attempts to connect to a backup TACACS+ server.

**Usage** Specify a number. The 0 (zero) default specifies that the Stinger unit does not attempt to connect to a backup TACACS+ server.

**Example** `set auth-retries = 2`

**Dependencies** For auth-retries to apply, you must set auth-type to tacacsplus.

**Location** `EXTERNAL-AUTH:tacplus-auth-client`

## auth-rsp-required

**Description** Specifies how the Stinger unit responds if an authentication request times out after a call has passed calling line ID (CLID) authentication.

**Usage** Specify one of the following settings:

- `yes` (the default)—Specifies that the Stinger unit drops calls that have passed CLID authentication.
- `no`—Specifies that the Stinger unit allows CLID-authenticated connections even if there is no response from the external server.

**Example** `set auth-rsp-required = yes`

**Dependencies** For auth-rsp-required to apply, CLID authentication must be in use, `clid-auth-mode` must be set to `required`, and `auth-type` must be set to `radius`.

**Location** `EXTERNAL-AUTH:rad-auth-client`

## auth-send67

**Description** Specifies whether the Stinger unit requires Remote Authentication Dial-In User Service (RADIUS) attributes 6 (User-Service) and 7 (Framed-Protocol) in a RADIUS user profile when a user wants to initiate PPP.

**Usage** Valid values are as follows:

- `yes`—Specifies that if a user wants to initiate PPP, his or her RADIUS profile must include attributes 6 and 7.
- `no`—Specifies that attributes 6 and 7 need not be present in a RADIUS user profile for a user to initiate PPP. This is the default.

**Example** `set auth-send67 = yes`

**Location** `EXTERNAL-AUTH:rad-auth-client`

## auth-server-n

**Description** Specifies the IP addresses of up to three external authentication servers.

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

**Usage** Specify an IP address in dotted decimal notation, separating the optional subnet mask value from the address with a forward slash (\). The addresses must all point to servers of the same type, as specified by the `auth-type` setting. The default is 0.0.0.0, which indicates that no authentication server exists.

**Example** `set auth-server-1 = 10.2.3.4/24`

**Location** `EXTERNAL-AUTH:rad-auth-client`  
`EXTERNAL-AUTH:tac-auth-client`  
`EXTERNAL-AUTH:tacplus-auth-client`

## auth-sess-interval

**Description** Specifies the number of seconds between RADIUS authentication reports concerning the number of open sessions.

**Usage** Specify a number of seconds from 0 through 65535. The 0 (zero) default turns off regular RADIUS open-session reports.

**Example** `set auth-sess-interval = 15`

**Dependencies** For `auth-sess-interval` to apply, you must set `auth-type` to `radius`.

**Location** `EXTERNAL-AUTH:rad-auth-client`

## auth-session-key

**Description** Specifies whether session-key assignments are enabled.

**Usage** Valid values are as follows:

- `yes`—Specifies that session-key assignments are enabled.
- `no`—Specifies that session-key assignments are disabled. This is the default.

**Example** `set auth-session-key = no`

**Dependencies** If `rad-serv-enable` is set to `no`, `auth-session-key` does not apply.

**Location** `EXTERNAL-AUTH:rad-auth-server`

## auth-src-port

**Description** Specifies the UDP source port to use for external authentication.

The Stinger unit uses the source port number to demultiplex the RADIUS reply packets to the appropriate modules. A separate source port is used for each module. On the Stinger unit, the actual source port is the value of auth-src-port plus the slot number, where the control module has a slot number of 0 (zero). So, if auth-src-port is set to 1000, packets originating from the control module have a source port value of 1000, while packets originating from slot 6 have a source port value of 1006.

**Usage** Specify a value from 0 to 65535. The default is 0 (zero), which specifies that the source port is selected from the nonprivileged port range (1024 through 2000).

**Example** set auth-src-port = 9000

**Location** EXTERNAL-AUTH:rad-auth-client  
EXTERNAL-AUTH:tac-auth-client  
EXTERNAL-AUTH:tacplus-auth-client

## auth-timeout

**Description** Specifies the number of seconds between attempts to reach an external authentication server.

The Stinger unit waits the specified number of seconds for a response to a RADIUS authentication request. If the Stinger unit does not receive a response within that time, it times out and sends the authentication request to the next authentication server (for example, auth-server-2).

**Usage** Specify an integer from 1 to 10. The default is 1 for a RADIUS request.

**Example** set auth-timeout = 5

**Dependencies** If auth-type is set to none, the auth-timeout parameter value does not apply.

**Location** EXTERNAL-AUTH:rad-auth-client  
EXTERNAL-AUTH:tac-auth-client

## auth-timeout-time

**Description** Specifies the number of seconds that must elapse before the Stinger unit attempts to connect to a backup TACACS+ server.

**Usage** Specify the number of seconds. The 0 (zero) default specifies that the Stinger unit does not attempt to use a backup TACACS+ server.

**Example** set auth-timeout-time = 60

**Dependencies** For auth-timeout-time to apply, you must set auth-type to tacacsplus.

**Location** EXTERNAL-AUTH:tacplus-auth-client

## auth-ts-secure

**Description** Specifies security access to the terminal-server interface when the RADIUS Login-IP-Host (14) value is not specified.

**Usage** Valid values are as follows:

- **yes**—Specifies that the terminal-server must be secure. If the Login-IP-Host is not specified, the Stinger unit drops the call. This is the default.
- **no**—Specifies that if the Login-IP-Host is not specified, the Stinger unit allows the dial-in connection to access the terminal-server interface.

**Example** `set auth-ts-secure = yes`

**Location** EXTERNAL-AUTH:rad-auth-client

## auth-type

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

**Usage** Valid values are as follows:

- **none**—Disables the use of an authentication server. This is the default.
- **radius**—Specifies that the Stinger unit accesses a RADIUS server. In a RADIUS query, the Stinger unit provides a user ID and password to the server. If the validation succeeds, the server sends back a complete profile. The profile specifies routing, destination-specific static routes, and usage restrictions for the user. RADIUS supports Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP), and terminal-server validation.
- **radius/logout**—Identical to radius, except that when you select radius/logout, the Stinger unit sends a request to the RADIUS server to initiate logout when the session ends.

**Example** `set auth-type = radius`

**Dependencies** If auth-type is set to a value other than none, you must specify at least one authentication server address.

**Location** EXTERNAL-AUTH

## auto-base-rate

**Description** Specifies the initial rate at which the SDSL LIMs train, in kilobytes per second.

**Usage** Specify one of the following rates:

144000  
272000 (the default)  
400000  
528000  
784000  
1168000  
1552000  
2320000

**Example** `set auto-base-rate = 272000`

**Dependencies** This parameter is ignored if `data-rate-mode` is set to `fastautobaud`.

**Location** `SDSL:line-config`

## auto-correction-enable

**Description** Specifies whether autocorrections for this line interface module (LIM) are enabled or disabled.

**Usage** Valid values are as follows:

- `no`—Specifies that the LIM attempts to correct problems every few hours automatically.
- `yes`—Specifies that the LIM uses the `interval-auto-correction` parameter to determine how often to correct itself. This is the default.

**Example** `set auto correction-enable = yes`

**Location** `SYSTEM-INTEGRITY:integrity-config`

## auto-logout

**Description** Specifies whether to log off the current user profile and go back to default privileges upon loss of a Data Transmit Ready (DTR) signal from the serial port.

**Usage** Valid values are as follows:

- `yes`—Specifies that the Stinger unit automatically logs off the current user profile if DTR is lost on the serial port.
- `no`—Specifies that the current user profile remains logged in. This is the default.

**Example** `set auto-logout = yes`

**Location** `SERIAL`

## auto-negotiate

**Description** Enables or disables negotiation by the LAN interface of its own operating speed and duplex mode.

**Usage** Valid values are as follows:

- *yes*—The interface determines the appropriate operating speed and duplex mode by using the autonegotiation protocol.
- *no*—The *duplex-mode* and *media-speed-mbit* settings determine operating speed and mode of the interface. This is the default.

**Example** `set auto-negotiate = yes`

**Location** `ETHERNET`

## auto-profile

**Description** Specifies whether the automatic creation of an accessory profile for ATM termination and the ATM circuit is enabled or disabled when the LAN session is established on an IDSL line interface module (LIM).

When PPP transparent circuit or frame relay circuit encapsulation is configured for connection profiles assigned to the Stinger unit IDSL LIM, the accessory profiles for ATM termination and the ATM circuit are *automatically* created by the system when the LAN session is established on the interface.

The accessory profiles are automatically created with the station name set to the station name of the parent PPP transparent circuit or frame relay circuit connection profile. The suffix `_SYXA` is added to the name of the accessory ATM termination profile, and the suffix `_SYXC` is added to the name of the ATM circuit profile.

**Usage** Valid values are as follows:

- *yes*—Specifies that automatic profile creation is enabled. This is the default.
- *no*—Specifies that automatic profile creation is disabled.

**Example** `set auto-profile = no`

**Dependencies** The ATM termination profile can be either ATM encapsulation or ATM frame relay circuit encapsulation. For automatic profiles, if the parent profile (which is the profile configured for PPP transparent circuit or frame relay circuit encapsulation), is modified or deleted, then the accessory profiles are deleted, if they exist.



**Note** A convenient way to delete the accessory profiles without deleting the parent profile is to set `auto-profile` to `no` while the parent profile is active.

**Location** `CONNECTION`

## auto-telnet

**Description** *Not used.*

## auto-update

**Description** Specifies whether regular successful Domain Name System (DNS) queries update the local DNS table. You can use this feature to build a DNS table stored in local RAM, to be used if DNS servers become unavailable.

When this feature is enabled and a DNS query succeeds, the system performs a lookup on that hostname in the local table. If no entry exists for the hostname, the entry's IP address (or multiple addresses) is replaced by the query response. The number of addresses added to the table depends on the `dns-list-attempt` and `dns-list-size` settings.

**Usage** Valid values are as follows:

- `yes`—Enables the auto-update feature for the DNS local table.
- `no`—Disables auto-update. The contents of the local DNS table are not affected by successful DNS queries. This is the default.

**Example** `set auto-update = yes`

**Dependencies** The `dns-list-attempt` and `dns-list-size` settings affect how the table is updated when `auto-update` is set to `yes`.

If `dns-list-attempt` is set to `yes`, a successful DNS query returns the number of addresses it finds for the host, up to the value of `dns-list-size`. In the DNS table in RAM, those addresses are stored, overwriting the configured address or the addresses retrieved from earlier DNS queries. If the table in RAM contains more addresses than `dns-list-size` specifies, the excess addresses are cleared at each update to prevent the accumulation of stale addresses.

**Location** `IP-GLOBAL:dns-local-table`

## aux-send-password

**Description** Specifies the password the Stinger unit sends when it adds channels to a Multilink Protocol Plus™ (MP+) call that uses PAP-Token-CHAP authentication. The unit obtains authentication of the first channel of the MP+ call from the user's hand-held security card.

**Usage** Enter the same password specified by `Ascend-Receive-Secret` in the RADIUS user profile for the Stinger unit.

**Example** `set aux-send-password = unit0`

**Dependencies** For `aux-send-password` to apply, the call must use MP+.

**Location** `CONNECTION:mpp-options`

## avcr-mt

**Description** Specifies the minimum threshold, expressed as a percentage, used in the algorithms that determine significant change for available cell rate (AvCR) parameters.

**Usage** Specify a percentage. The default is 3 percent.

**Example** `set avcr-mt = 3`

**Location** PNMI-NODE-CONFIG:node-timer

## avcr-pm

**Description** Specifies the proportional multiplier, expressed as a percentage, used in the algorithms that determine significant change for available cell rate (AvCR) parameters—for example, increase by 50 percent, or decrease by 50 percent.

Available cell rate specifications use a proportional multiplier.

**Usage** Specify a percentage. The default is 50 percent.

**Example** `set avcr-pm = 50`

**Location** PNMI-Node-Config[n]:node-timer

## B

## background-noise-filter

**Description** Specifies the type of filter to use for background noise tests performed with the copper loop test (CLT) module.

**Usage** Valid values are as follows:

- `psd`—Power spectral density measurement for a 22KHz-to-1.6Mhz range. This is the default.
- `e`—Reports one noise value at 135-ohm impedance for a 1KHz-to-50kHz range. Used for ISDN qualification.
- `f`—Reports one value for a 5KHz-to-245KHz range. Used for HDSL qualification.
- `g`—Reports one noise value at 100-ohm impedance for a 20KHz-to 1.1-MHz range. Used for ADSL qualification.

**Example** `set background-noise-filter = psd`

**Location** CLT-COMMAND



## background-noise-termination

**Description** Sets the receiver termination for a background noise test performed with the copper loop test (CLT) module.

**Usage** Valid values are as follows:

- `term100`—Places a 100-ohm termination on the received signal. This is the default.
- `term135`—Places a 135-ohm termination on the received signal.
- `bridge100`—Puts the receiver in high-impedance mode, and calculates a noise signal based on 100-ohm impedance.
- `bridge135`—Puts the receiver in high-impedance mode, and calculates a noise signal based on 135-ohm impedance.

**Example** `set background-noise-termination = bridge135`

**Location** `CLT-COMMAND`

## backup

**Description** Specifies the name of a backup connection profile for a dedicated (nailed) connection. The profile serves as a backup if the remote device goes out of service. It is not intended to provide alternative lines for getting to a single destination.

When the system detects that the primary interface is unavailable, it puts the primary interface in a Backup Active state. *It does not remove the routes to the primary interface.* It then diverts traffic from the primary to the backup interface. When the system detects that the primary interface is available again, it diverts traffic back to the primary interface. If the backup interface is a switched connection, the Stinger unit then breaks the connection.

**Usage** Specify the name of a connection profile. You can enter up to 32 characters. The default is null.

**Example** `set backup = newyork`

**Dependencies** Consider the following:

- One of the side effects of the data-link-layer backup interface is that, when a dedicated (nailed) interface specifies a backup interface, the routes to the dedicated interface never go down.
- Nested backups are not supported. (The profile for a backup interface cannot specify another backup interface.)
- The profile for a backup interface does not inherit attributes from the profile for the primary dedicated connection.

**Location** `CONNECTION:session-options`

## backup-enabled

**Description** Read-only. Internal field used with backup profiles.

**Usage** Read-only parameter with the following values:

- no—Backup is disabled.
- yes—Backup is enabled.

**Example** backup-enabled = yes

**Location** CONNECTION:session-options

## bad-count

**Description** Read-only. Indicates the number of times this device has failed.

**Usage** Read-only numeric value with range 0 to 4294967295.

**Example** bad-count = 96

**Location** DEVICE-STATE

## bandwidth

**Description** Specifies the shaped bandwidth in kilobits per second.

**Usage** Valid values range from 8000Kbps through 148598Kbps. The default is 8000.

**Example** set bandwidth = 9000

**Location** SWITCHCONFIG:atm-parameters:outgoing-shaper:outgoing-shaper [n]

## bandwidth-monitor-direction

**Description** Specifies the direction for monitoring link utilization.

**Usage** Valid values are as follows:

- transmit—Monitors the transmit direction only.
- transmit-recv—Monitors both the transmit and receive directions.
- none—Turns off link utilization monitoring.

**Example** set bandwidth-monitor-direction = transmit

**Location** ANSWER-DEFAULTS:mp-answer  
CONNECTION:mpp-options

## banner

**Description** *Not used.*

banner [n]

**Description** *Not used.*

base-channel-count

**Description** Specifies the number of channels to be used for a call when the session is initially set up, provided that it is a fixed session.

**Usage** Specify a number between 0 (zero) and 65535. The default is 1 (one).

**Example** `set base channel count = 25`

**Location** CONNECTION:mp-options

base-udp-port

**Description** Specifies a UDP port number. The default zero value causes the system to dynamically assign a nonprivate port for exchanging control information while establishing a tunnel. Having a nonprivate port avoids the possibility of requesting a UDP port that is already in use.

**Usage** You can configure nonzero values from 10,000 to 60,000 to use a known port, which is sometimes a firewall requirement. The system uses the configured value in the following formula to assign a port number:

`base-udp-port + (shelf-number × 100) + slot-number`

**Example** `set base-udp-port = 55555`

**Location** L2-TUNNEL-GLOBAL:l2tp-config

ber-receive

**Description** Read-only. Indicates whether the bit-error-rate threshold has been reached or not.

**Usage** Valid values for this read-only parameter are as follows:

- `true`—Indicates that the bit-error-rate threshold has been reached.
- `false`—Indicates that the bit-error-rate has not been reached.

**Example** `ber-receive = false`

**Location** DS1-ATM-STAT  
T1-STAT

## bert-enable

**Description** Specifies whether the bit-error-rate test (BERT) is enabled or disabled.

To check the data integrity of the connection, the BERT counts data errors that occur on each channel. If the two ends of the connection are physically connected, the BERT is run between the two units. If the two ends are not connected, the BERT is run within the module itself. Both ends of the connection must enable the BERT.



**Note** During a BERT, normal data transmission is interrupted.

**Usage** Valid values are as follows:

- yes—Enables the BERT.
- no—Disables the BERT. This is the default

**Example** `set bert-enable = yes`

**Dependencies** Consider the following:

- The `bert-enable` setting is not saved to the unit's permanent memory. If you reset the module or the unit, the setting reverts to its default.
- The `bert-timer` setting determines the duration of the BERT.

**Location** `LINE-DIAG`

## bert-error-counter

**Description** Read-only. Indicates the number of errors received during the bit-error-rate test (BERT).

**Usage** The `bert-error-counter` parameter is read-only.

**Dependencies** You must set `bert-enable` to `yes` for `bert-error-counter` to apply.

**Example** `bert-error-counter = 0`

**Location** `LINE-DIAG-STAT`

## bert-operation-state

**Description** Read-only. Indicates the state of the bit-error-rate test (BERT).

**Usage** The `bert-operation-state` setting is read-only. Valid values are as follows:

- `waiting-for-511-sync`—The Stinger unit is waiting for customer premises equipment (CPE) before starting the BERT.
- `local-loop-active`—The interface is in local analog loopback and is running the test. No remote device is involved.
- `active`—BERT is running with customer premises equipment (CPE).
- `stopped`—BERT was disabled.
- `loop-back-setup`—The interface is being placed into analog loopback.
- `start-up`—BERT is starting up.

**Example** `bert-operation-state = stopped`

**Dependencies** If the two ends of the connection are not connected, the `bert-operation-state` setting does not apply. In this case, you must set `bert-enabled` to `no` to end the BERT.

**Location** `LINE-DIAG-STAT`

## `bert-timer`

**Description** Specifies the duration of a bit-error-rate test (BERT).

**Usage** Specify one of the following values:

- 1 minute (the default)
- 2 minutes
- 3 minutes
- 4 minutes
- 5 minutes
- 10 minutes
- 15 minutes
- 20 minutes
- 30 minutes

**Example** `set bert-timer = 1 minute`

**Dependencies** Consider the following:

- If the two ends of the connection are not connected, `bert-timer` does not apply. In this case, you must set `bert-enabled` to `no` to end the BERT.
- The `bert-timer` setting is not saved to the unit's permanent memory. If you reset the module or the unit, the setting reverts to its default.

**Location** `LINE-DIAG`

## `beta-ima-value`

**Description** Specifies the beta value used to specify the number of consecutive invalid IMA Control Protocol (ICP) cells to be detected before moving to inverse multiplexing over ATM (IMA) HUNT state from the SYNC state.

**Usage** Valid numbers range from 1 to 5. The default is 2.

**Example** `set beta-ima-value = 2`

**Location** `IMAHW-CONFIG`

## bi-directional-auth

**Description** Specifies whether Challenge Handshake Authentication Protocol (CHAP) authentication must be bidirectional. If bidirectional CHAP is allowed or required, and the second authentication is attempted, it must be successful. Otherwise, the Stinger unit rejects the call.

**Usage** Specify one of the following values:

- **none** (the default)—CHAP authentication is unidirectional. The system identifies the calling device.
- **allowed**—Authentication can be bidirectional. The system identifies the calling device, and also allows the calling device to authenticate the Stinger unit. The system tries to negotiate authentication in the opposite direction as well, but the call is established even if the called device refuses to perform the second authentication option.
- **required**—Authentication must be bidirectional. The system requires that both the calling and called devices authenticate each other. If authentication is not performed in both directions, the Stinger unit rejects the call.

**Example** `set bi-directional-auth = allowed`

**Dependencies** Bidirectional authentication is applicable only if the authentication mode is CHAP, MS-CHAP, or cache-token-ppp-auth. If receive-auth-mode is set to any-ppp-auth and the system negotiates Password Authentication Protocol (PAP) authentication with the caller, bidirectional authentication is automatically disabled, even if bi-directional-auth is set to required.

**Location** ANSWER-DEFAULTS:ppp-answer  
CONNECTION:ppp-options

**See Also** ppp-answer, ppp-options

## billing-number

**Description** *Not supported.* Specifies a telephone number provided by the carrier to be used for billing purposes.

**Location** CALL-INFO  
CONNECTION:telco-options  
FRAME-RELAY

## bin-loading

**Description** An array that enables or disables up to 256 bins (intervals) that correspond to particular frequencies.

**Usage** For each element in the array, specify one of the following values:

- **yes** (the default)—Enables a bin to allow a frequency.
- **no**—Disables a bin to mask a frequency.

To determine the bin number in the array, divide the frequency in question by 4.3125 and add 1.

**Example** The following command masks the frequency 640kHz by disabling bin 149 ( $640/4.3125 + 1 = 149$ ):

```
set bin-loading 149 = no
```

**Location** ADSL-BIN-LOADING

## bin-loading-profile

**Description** Specifies the name of the adsl-bin-loading profile that applies to this ADSL line.

**Usage** Specify the name of a bin-loading profile. By default, the bin-loading-profile parameter takes the settings of the adsl-bin-loading profile, default.

**Example** `set bin-loading-profile = default`

**Location** AL-DMT

## bit-rate

**Description** Specifies the maximum sustainable effective bit rate in kilobits per second.

**Usage** The valid range is 1 through 135631. The default is 1000 (1Mbps). The Stinger unit verifies that the bit-rate value of a shaper does not exceed the effective line rate.

**Example** `set bit-rate = 10000`

**Location** SYSTEM:traffic-shaper  
ATM-INTERNAL:traffic-shapers [n]

## bits-per-bin

**Description** Specifies the maximum number of bits per frequency bin (interval).

**Usage** Although you can specify a number from 0 through 15, leave this parameter at its default setting of 14, unless you encounter the following situations:

- You need to restrict the line rate, but at the same time retain a uniform distribution of bits per bin across all the bins.
- You need to lower the bits per bin to enable the Stinger unit to interoperate with customer premises equipment (CPE) devices that do not allow 14 bits per bin.

**Example** `set bits-per-bin = 10`

**Location** ADSL-BIN-LOADING

## bit-strings-allowed

**Description** Specifies whether the SNMP agent in a Stinger unit responds to the BITS data type in bit string format or numeric format.

**Usage** Valid values are as follows:

- **yes** (the default)—Specifies that the SNMP agent responds to BITS data in bit string format.
- **no**—Specifies that the SNMP agent responds to BITS data in numeric format.

**Example** `set bit-strings-allowed = no`

**Location** `SNMP`

## bit-swapping

**Description** Enables or disables bit swapping for an ADSL line interface module (LIM).



**Note** On the 48-port ADSL G.lite LIM, bit swapping has no effect.

**Usage** Valid values are as follows:

- **yes**—Specifies that bit swapping is enabled
- **no**—Specifies that bit swapping is disabled. This is the default.

**Example** `set bit-swapping = yes`

**Location** `AL-DMT:line-config`

## boot-cm-version

**Description** Read-only. Indicates the version of the control module (CM) boot loader currently present on the control module.

**Usage** Read-only, 20-character, alphanumeric field.

**Example** `boot-cm-version = 9.2-167.0`

**Location** `SYSTEM`

## bootp-enabled

**Description** Enables or disables querying a BOOTP server for settings or to check for a new software load.

**Usage** Specify one of the following values:

- **yes**—Enables the system to use BOOTP.
- **no**—Disables the use of BOOTP. This is the default.

**Example** `set bootp-enabled = yes`

**Location** `IP-GLOBAL`



`bootp-servers [n]`

**Description** An array that specifies the IP address of a BOOTP server.

Multiple DHCP servers are not supported.

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

**Example** `set 1 = 12.34.56.78`

**Location** `IP-GLOBAL:bootp-relay`

`bottom-high-temperature-threshold`

**Description** *Not supported.* Specifies the bottom control module (CM) thermal sensor high temperature trigger level (in degrees Celsius). When the temperature exceeds this value, an alarm or watchdog state can be generated.

**Usage** Specify a numeric value between -20 degrees C and 75 degrees C (-4 degrees F and 167 degrees F). A value of 60 degrees C (140 degrees F) is the default.

**Example** `set bottom-high-temperature-threshold = 65`

**Dependencies** This threshold can be used for setting an alarm profile and `watchdog-config` profile trap. Temperature sensors are available only in version 3 and higher of the CM.

**Location** `THERMAL`

`bottom-low-temperature-threshold`

**Description** *Not supported.* Specifies the bottom control module (CM) thermal sensor low temperature trigger level (in degrees Celsius). When the temperature falls below this value, an alarm or watchdog state can be generated.

**Usage** Specify a numeric value between -20 degrees C and 75 degrees C (-4 degrees F and 167 degrees F). A value of 0 degrees C (32 degrees F) is the default.

**Example** `set bottom-low-temperature-threshold = 15`

**Dependencies** This threshold can be used for setting an alarm profile and `watchdog-config` profile trap. Temperature sensors are available only in version 3 and higher of the CM.

**Location** `THERMAL`

## bottom-status

**Description** Specifies the default contents of the bottom-right portion of the status window.

**Usage** Valid values are as follows:

- `general-info`—Displays general information and statistics for the system.
- `log-window`—Displays saved system-event log entries. This is the default.
- `line-status`—Displays the status of the system telephony interfaces.

**Example** `set bottom-status = general-info`

**Location** USER

## bpv-error-count

**Description** Read-only. Indicates the number of bipolar violation (BPV) errors received since the last time the unit was reset. BPV errors might indicate that the line sent consecutive 1 (one) bits with the same polarity, that three or more consecutive zeroes were sent, or that an incorrect polarity was present.

**Usage** The `bpv-error-count` value is read-only.

**Example** `bpv-error-count = 0`

**Location** DS3-ATM-STAT  
E3-ATM-STAT

## bridge

**Description** Enables or disables ethernet bridging on the interface. With ethernet bridging, the Stinger unit can provide a connection between segments that might be connected by a telecommunications link.

**Usage** Valid values are as follows:

- `yes`—Enables ethernet bridging.
- `no` (the default)—Does not enable ethernet bridging.

**Example** `set bridge = yes`

**Dependencies** In the `ETHERNET:bridging-options` profile this number is not used for VLAN bridging.

**Location** CONNECTION:bridging-options  
ETHERNET:bridging-options  
VLAN-ETHERNET:bridging-options

## bridge-non-pppoe

**Description** Enables or disables bridging of packets other than PPP over Ethernet (PPPoE) packets on the interface.

**Usage** Valid values are as follows:

- `yes`—Bridges all types of bridged packets.
- `no` (the default)—Bridges only PPPoE packets and discards other types of bridged packets.

**Example** `set bridge-non-pppoe = yes`

**Dependencies** Setting `bridge-non-pppoe = yes` will have no effect unless the parameter `bridging-enabled` in the corresponding ethernet profile is set to `yes`.

**Location** `CONNECTION:pppoe-options`  
`ETHERNET:pppoe-options`

## bridge-status

**Description** Read-only. Indicates the status of the bridge in the automatic protection switching (APS) system.

**Usage** Valid values for this read-only parameter are as follows:

- `true`—Bridging is enabled. Bridging is always enabled when the APS system is enabled in 1+1 protection mode.
- `false`—Bridging is disabled.

**Example** `bridge-status = true`

**Location** `APS-STAT`

## bridge-tap-length

**Description** Read-only. Indicates the loop length to the first bridge tap detected by the copper loop test (CLT) module.

**Usage** Read-only numeric field 0 to 4294967295.

**Example** `bridge-tap-length = 3500`

**Dependencies** This value is reported in feet if `TDR units` is set to `english`, or in meters if `TDR units` is set to `metric`.

**Location** `CLT-RESULT`

## bridge-tap-number

**Description** Read-only. Indicates the number of bridge taps detected by the copper loop test (CLT) module.

**Usage** Read-only numeric field 0 to 4294967295.

**Example** bridge-tap-number = 3

**Location** CLT-RESULT

## bridge-tap-table

**Description** Read-only. Indicates the sets of three values of bridge tap data. One set of values is reported for each bridge tap detected.

**Usage** Read-only parameters. Each set of data contains the following values:

- Bridge-tap distance in feet or meters.
- Bridge-tap length in feet or meters.
- Confidence level in percentage. Valid values are 33 or 50%.

**Dependencies** The current copper loop test (CLT) module hardware supports only a single set of bridge-tap data.

**Location** CLT-RESULT

## bridge-type

**Description** Type of bridging.

**Usage** Valid values are as follows:

- transparent-bridging—Default value.
- no-bridging—Bridging disabled.
- vlan-circuit—Required for 1:1 VLAN bridging.
- stacked-vlan—Required for VLAN stacking.

**Example** set bridge-type = transparent-bridging

**Dependencies** This parameter's setting is ignored for ethernet profiles on the IP2000 and Fast Ethernet circuit packs. The default transparent-bridging setting is always used.

**Location** CONNECTION:bridging-options  
ETHERNET:bridging-options  
VLAN-ETHERNET:bridging-options

## bridging-enabled

**Description** Enables or disables Ethernet bridging or VLAN bridging on the Ethernet interface.

**Usage** Valid values are as follows:

- **yes**— Enables Ethernet bridging or VLAN bridging or both.
- **no** (the default)—Disables both Ethernet bridging and VLAN bridging. The system does not accept unicast packets received on this port unless the destination MAC address is equal to the MAC address of the port.

**Example** `set bridging-enabled = yes`

**Location** `ETHERNET`

## bridging-group

**Description** Specifies a number used to group bridged interfaces. When multiple bridged interfaces use the same group number, the Stinger unit consults the bridge logic for a destination interface only within that group. Bridged interfaces that use a different group number are not considered. The effect is to isolate traffic within a bridging group.

In the `answer-defaults` profile, this parameter specifies a default bridging group to use for PPP session requests that do not specify a group number in the `connection` or `radius` profile.



**Note** For performance reasons, specifying a unique nonzero bridging-group value on a PPPoE interface is recommended. A unique group guarantees that packets do not flow between two bridged interfaces.

**Usage** Specify a group number from 0 to 65535. The default value is 0 (zero) and disables bridging.

**Example** `set bridging-group = 1`

**Dependencies** See the configuration guide for each respective circuit pack for specific dependencies.

**Location** `ANSWER-DEFAULTS:ppp-answer`  
`BRIDGE-GROUP`  
`CONNECTION:bridging-options`  
`ETHERNET:bridging-options`  
`VLAN-ETHERNET:bridging-options`

## btap-measure-length

**Description** Specifies the loop length—100 to 20000 feet (32 to 6097 meters)—for a bridge-tap search by the copper loop test (CLT) module.

**Usage** Specify a number between zero (0) and 65535. The default is zero.

**Example** `set btap-measure-length = 100`

**Location** CLT-COMMAND

## btap-start-length

**Description** Specifies the starting location—15 to 20000 feet (5 to 6097 meters)—for a bridge-tap search by the copper loop test (CLT) module.

**Usage** Specify a number between zero (0) and 65535. The default is zero.

**Example** `set btap-start-length = 50`

**Location** CLT-COMMAND

## buffer-chars

**Description** *Not used.*

## C

## cac-preference

**Description** Specifies whether the system reserves bandwidth for a connection at connection setup time or when the connection is provisioned.

**Usage** Valid values are as follows:

- `connection-time` (the default)—The system attempts to reserve bandwidth for a connection when it is establishing the connection.
- `provisioning-time`—The system attempts to reserve bandwidth for a connection when it is provisioning the connection. You can configure a new connection or modify an existing one only if there is sufficient available bandwidth.

**Example** `set cac-preference = provisioning-time`

**Dependencies** Consider the following:

- A change in the `cac-preference` value takes effect only after a system reset.
- When you modify the quality-of-service (QoS) definitions in an `atm-qos` profile, all connection profiles (both active and inactive) that specify the use of that profile are affected. The system deallocates the bandwidth assigned to those connections and then reallocates it according to the new definitions in the `atm-qos` profile.



**Note** If it does not have sufficient bandwidth for all connections, the system allocates the guaranteed bandwidth for as many connections as possible. The remaining connections (if any) that use the modified `atm-qos` profile are allocated no bandwidth and are therefore not established.

- With `provisioning-time` in effect, if CAC bandwidth allocation fails while the system is provisioning a new connection or modifying the `nailed-group` or `atm-qos` profile assignment of an existing connection profile, the system displays an error message and does not write the profile. When the system fails to modify an existing configuration due to lack of sufficient available bandwidth, the existing CAC bandwidth is maintained for the connection.

**Location** `SYSTEM`

## calea

**Description** Indicates whether the Communications Assistance for Law Enforcement Act (CALEA) license is enabled.

**Usage** The `calea` setting is read-only and can have one of the following values:

- `yes` indicates that the CALEA license is enabled.
- `no` indicates that the CALEA license is not enabled.

**Example** `calea = yes`

**Location** `BASE`

## calibration-type

**Description** Specifies the type of calibration needed for certain copper loop test (CLT) module tests.

**Usage** Specify one of the following values:

- insertion-loss (the default)—Calibration type for an insertion loss test.
- background-noise—Calibration type for a background noise test.

**Example** set calibration-type = insertion-loss

**Location** CLT-COMMAND

## callback

**Description** *Not supported.* Enables or disables callback security, which requires dial-out capability.

**Usage** Valid values are as follows:

- yes
- no (the default)

**Location** CONNECTION:telco-options

## call-by-call

**Description** *Not used.*

**Location** CALL-INFO

## call-by-call-id

**Description** *Not used.*

**Location** FRAME-RELAY

## callednumber

**Description** *Not supported.* Specifies the number called to establish the connection used for dialed number identification service (DNIS) authentication.

**Location** CONNECTION

## called-number-type

**Description** *Not supported.* Specifies the type of telephone number used to dial a call.

**Location** CALL-INFO

CONNECTION

FRAME-RELAY



## call-filter

**Description** Specifies the name of a filter to apply to the interface. The filter name can be from a local filter profile or RADIUS pseudo-user profile.

The setting in the answer-defaults profile is used only for RADIUS-authenticated connections that do not specify a call filter.

If the system applies both a call filter and a data filter to a connection, it applies the data filter first. Only those packets that the data filter forwards reach the call filter.

**Usage** Specify the filter name. The default is null, which indicates no filter.

**Example** `set call-filter = test`

**Dependencies** If a local connection profile does not use authentication, it cannot specify a RADIUS filter profile. *Filters are not supported with the current software version.*

**Location** ANSWER-DEFAULTS:session-info  
CONNECTION:session-option

## call-info

**Description** Specifies whether, at the time an authenticated call ends, the Stinger unit reports to syslog the following information about the call:

- Station name
- Calling telephone number
- Called telephone number
- Encapsulation protocol
- Data rate (in bits per second)
- Progress code or disconnect reason
- Number of seconds before authentication
- Number of bytes or packets received during authentication
- Number of bytes or packets sent during authentication
- Length of session (in seconds)
- Number of bytes or packets received during the session
- Number of bytes or packets sent during the session

A one-line syslog message contains information about the terminated call. The information also appears in the connection status window and is logged as a message at level INFO. For example:

```
"Conn= ("cjones-p50" 5106785291->? MP 56000 60/185) \
Auth=(3 347/12 332/13) \
Sess=(1 643/18 644/19), Terminated"
```

If some of the information is not available, that field is displayed as either a question mark (?) for strings or a zero (0) for numerals.



**Note** Use call-info only for diagnosing session problems. Because the reports to syslog rely on the UDP protocol, which does not guarantee delivery, do use call-info for billing purposes.

**Usage** Valid values are as follows:

- `end-of-call`—Specifies that the Stinger unit reports the information to `syslog`.
- `none` (the default)—Specifies that the Stinger unit does not report the information.

**Example** `set call-info = end-of-call`

**Location** `LOG`

## `calling-integrity-time`

**Description** *Not used.* Specifies the number of seconds a node waits for an switched virtual channel connection (SVCC) it has initiated to become fully established before giving up and tearing it down.

**Location** `PNMI-NODE-CONFIG:node-svcc-rcc`

## `call-kind`

**Description** Specifies the type of call control for an ATM virtual path link (VPL) or virtual channel link (VCL) configuration.

**Usage** Specify one of the following call control types:

- `pvc`—Virtual link of a permanent virtual circuit (PVC) or permanent virtual path (PVP). This is the default value.
- `svc-incoming`—Virtual link established after reception of a signaling request to set up a switched virtual circuit (SVC). An `svc-incoming` type call is built dynamically.
- `svc-outgoing`—Virtual link established after the forwarding or transmission of a signaling request to set up an SVC. An `svc-outgoing` type call is built dynamically.
- `spvc-initiator`—Virtual link at the PVC side of an SVC or PVC cross-connect, where the switch is the initiator of the soft PVC (SPVC) setup.
- `spvc-target`—Virtual link at the PVC side of an SVC or PVC cross-connect, where the switch is the target of the soft PVC setup. An `spvc-target` type call is built dynamically.

**Location** `ATM-VCL-CONFIG`

`ATM-VPL-CONFIG`

## call-log-connection-packets-enable

**Description** Specifies that call-logging Start and Stop packets are sent when a connection is established or ended, in contrast to line statistics call logging, which is always enabled.

**Usage** Valid values are as follows:

- **yes**—Specifies that call-logging Start and Stop packets are sent when a connection is established or ended.
- **no** (the default)—Specifies that call-logging Start and Stop packets are not sent. To optimize operations use the default.

**Example** `set call-log-connection-packets-enable = yes`

**Location** `CALL-LOGGING`

## call-log-dropped-pkt-enabled

**Description** Enables or disables the transmission of an SNMP notification (trap) when the system detects a change in the status of call-logging packets.

If this parameter is enabled, the system generates a trap when the value of `callLoggingDroppedPacketCount` in the call-logging MIB changes. A change from 0 to 1 indicates that packets are being dropped. A change from 1 to 0 indicates that packets are no longer being dropped.

**Usage** Valid values are as follows:

- **yes** (the default)—Enables transmission of a notification when the system detects a change in the status of call-logging packets.
- **no**—Disables transmission of a notification when the system detects a change in the status of call-logging packets.

**Example** `set call-log-dropped-pkt-enable = no`

**Location** `TRAP`

## call-log-enable

**Description** Enables or disables call logging.

**Usage** Valid values are as follows:

- **yes**—Enables call logging.
- **no**—Disables call logging. This is the default.

**Example** `set call-log-enable = yes`

**Dependencies** If you set `call-log-enable` to `yes`, you must specify the IP address of at least one call-log host for the `call-log-host-n` setting.

**Location** `CALL-LOGGING`

call-log-evaluation-end-julian-time

**Description** *Internal use only.*

call-log-host-1

call-log-host-2

call-log-host-3

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

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

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

**Example** `set call-log-host-1 = 10.1.2.3`

**Dependencies** Consider the following:

- For call-log-host-1, call-log-host-2, or call-log-host-3 to apply, you must set call-log-enable to yes.
- Call logging is available with NavisRadius™ only. For information, see the NavisRadius™ documentation.

**Location** CALL-LOGGING

call-log-id-base

**Description** Specifies whether the Stinger unit presents a session ID to the call-log host in base 10 or base 16.

**Usage** Valid values are as follows:

- acct-base-10—Specifies a decimal base. This is the default.
- acct-base-16—Specifies a hexadecimal base.

**Example** `set call-log-id-base = acct-base-16`

**Dependencies** Consider the following:

- If call-log-enable is set to no, call-log-id-base does not apply.
- Changing the value of call-log-id-base while call-logging sessions are active results in inconsistent reporting between the Start and Stop records.

**Location** CALL-LOGGING

## call-log-key

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

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

**Example** `set call-log-key = mypw`

**Dependencies** If `call-log-enable` is set to `no`, `call-log-key` does not apply.

**Location** `CALL-LOGGING`

## call-log-limit-retry

**Description** Specifies the maximum number of retries for call-logging packets.

When the Stinger unit is configured for call logging, it sends Start and Stop packets to the call-log host to record connections. If the host does not acknowledge a packet within the number of seconds you specify for `call-log-timeout`, the Stinger unit tries again, resending the packet until the host responds, or dropping the packet if the queue of packets to be resent is full. You can limit the number of retries by setting a maximum.

The Stinger unit always makes at least one attempt before this parameter setting goes into effect. For example, if you set the number of retries to 10, the Stinger unit makes 11 attempts: the original attempt plus 10 retries.

**Usage** To set the maximum number of retries for Start and Stop packets, set `call-log-limit-retry` to a value greater than 0 (zero). A value of 0 (the default) indicates an unlimited number of retries.

**Example** `set call-log-limit-retry = 10`

**Location** `CALL-LOGGING`

## call-log-multi-packet

**Description** Enables or disables delivery by the Stinger unit of multiple requests in a single call-logging packet to a call-logging host that supports the Lucent 16-bit vendor-specific attributes (VSAs). Enabling this feature optimizes the transfer of call-logging data to the network management station.

**Usage** Valid values are as follows:

- `yes`—Specifies that multiple all-logging requests are sent in a single packet.
- `no` (the default)—Specifies that multiple all-logging requests are not sent in a single packet.

**Dependencies** This parameter can be enabled only if the `call-log-radius-compat` parameter is set to the value `16-bit-vendor-specific`.

**Example** `set call-log-multi-packet = no`

**Location** `CALL-LOGGING`

## call-log-port

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

**Usage** Specify a UDP port number from 1 to 32767. The value must match the port number configured on the call-logging host. The default is 1646.

**Example** `set call-log-port = 1500`

**Dependencies** If `call-log-enable` is set to `no` in the call-logging profile, `call-log-port` does not apply.

**Location** `CALL-LOGGING`

## call-log-radius-compat

**Description** Enables or disables vendor-specific attribute (VSA) compatibility mode when the unit is using RADIUS for call logging to the NavisAccess™ manager.

**Usage** Valid values are as follows:

- `vendor-specific`—Specifies 8-bit VSA support. All standard attributes are sent in standard RFC format, and all VSAs are sent in 8-bit VSA format. The unit ignores all VSAs in received packets that do not have `vendor-id` set to `ascend-vendor-id`.
- `16-bit-vendor-specific`—Specifies 16-bit VSA support. All standard attributes are sent in standard RFC format, and all VSAs are sent in the 16-bit VSA format as Lucent VSAs. The system ignores all VSAs in received packets that do not have `vendor-id` set to `lucent-vendor-id`. In this format, the first 256 Lucent VSAs are mapped to the 256 Ascend VSAs.



**Note** The `old-ascend` setting is no longer available for `call-log-radius-compat`.

**Example** `set call-log-radius-compat = vendor-specific`

**Dependencies** Consider the following:

- For `call-log-radius-compat` to apply, you must set `call-log-enable` to `yes`.
- Call logging is available with NavisRadius™ only. For information, see the NavisRadius™ documentation.
- At this time, only NavisRadius™ supports 16-bit VSAs.

**Location** `CALL-LOGGING`

## call-log-reset-time

**Description** Specifies the number of seconds that must elapse before the Stinger unit returns to using the primary call-log host (`call-log-host-1`).

**Usage** Specify the number of seconds. The default is 0 (zero), which specifies that the Stinger unit does not return to using the primary call-log host.

**Example** `set call-log-reset-time = 60`

**Dependencies** For `call-log-reset-time` to apply, you must set `call-log-enable` to `yes` in the call-logging profile and specify at least one value for `call-log-host-n` in the same profile.

**Location** `CALL-LOGGING`

## call-log-serv-change-enabled

**Description** Enables or disables trap (notification) generation when the call-logging server changes (Ascend trap 38).

If the call-logging server index is changed, or if the IP address of the active call-logging server is changed, this trap sends the following information to the Simple Network Management Protocol (SNMP) manager:

- The new call logging server index (`callLoggingServerIndex`)
- The IP address of new call logging server (`callLoggingServerIPAddress`)
- The absolute time to show when the server change occurred (`sysAbsoluteCurrentTime`)

**Usage** Specify one of the following settings:

- `yes`—Specifies that the unit generates a trap when the call-logging server changes.
- `no` (the default)—Specifies that the unit does not generate a trap when the call-logging server changes.

**Example** `set call-log-serv-change-enabled = yes`

**Dependencies** Call logging is available with NavisRadius™ only. For information, see the NavisRadius™ documentation.

**Location** `TRAP`

## call-log-server-index

**Description** Specifies which of the configured `call-log-host-n` parameter settings are used as the active call-logging server.

**Usage** Valid values are as follows:

- `host-1` (the default)
- `host-2`
- `host-3`

If the Stinger unit cannot authenticate the specified server, it attempts to use the next configured server.

**Example** `set call-log-server-index = host-1`

**Location** `CALL-LOGGING`

## call-log-stop-only

**Description** Specifies whether the Stinger unit sends a Stop packet that does not contain a username. (At times, the Stinger unit can send a Stop packet to the call-logging host without having sent a Start packet. Such a Stop packet has no username.)

**Usage** Valid values are as follows:

- **yes** (the default)—Specifies that the Stinger unit sends a Stop packet even if it does not contain a username. This is the default.
- **no**—Specifies that the Stinger unit does not send a Stop packet that does not contain a username.

**Example** `set call-log-stop-only = no`

**Location** `CALL-LOGGING`

## call-log-stream-period

**Description** Specifies the number of minutes between snapshots for stream packets.

**Usage** Leave the setting for this parameter at its default value of 15.

**Example** `set call-log-stream-period = 15`

**Location** `CALL-LOGGING`

## call-log-timeout

**Description** Specifies the amount of time (in seconds) that the Stinger unit waits for a response to a call-logging request. If it does not receive a response within the specified time, the Stinger unit sends the request to the next host specified by Call-Log-Host-N. If all call-logging hosts are busy, the Stinger unit stores the request and tries again at a later time. It can queue up to 154 requests.

**Usage** Specify an integer from 1 to 10. The default is 1.

**Example** `set call-log-timeout = 5`

**Dependencies** If `call-log-enable` is set to `no`, `call-log-timeout` does not apply.

**Location** `CALL-LOGGING`



## call-route-info

**Description** *Not used.* The current default setting indicates the preferred-source setting in a call-route profile. Any call received on the specified T1 channel is routed to the index address.

The preferred method of call routing is to use the call-route profile. However, although call-route-info is deprecated, any nondefault setting you specify for it takes precedence over a preferred-source specification in a call-route profile.

**Usage** Specify a device address within the Stinger unit. Set call-route-info in any profile or subprofile listed in the location information below. The default indicates any device and passes the responsibility for call routing to call-route profiles. Lucent Technologies recommends that you accept the default.

**Example** `set call-route-info = { 1 6 48 }`

**Location** AL-DMT:line-config  
DS3-ATM:line-config  
E3-ATM:line-config  
HDSL2:line-config  
OC3-ATM:line-config  
SDSL:line-config  
SHDSL:line-config

## call-route-type

**Description** Specifies the type of call that the Stinger unit can route to a host device.

**Usage** Valid values are as follows:

- any-call-type (the default)—Specifies that the Stinger unit can route any type of call to a host device.
- voice-call-type—Specifies that the Stinger unit can route voice bearer calls, excluding 3.1kHz audio, to a host device.
- digital-call-type—Specifies that the Stinger unit can route general digital calls, including 3.1kHz audio bearer channel calls, to a host device. As far as the Stinger unit is concerned, 3.1kHz audio calls are voice-bearing. The Stinger unit routes them to a modem, not a High-Level Data Link Control (HDLC) controller.
- trunk-call-type—Specifies that the Stinger unit routes calls to a trunk device. This value applies to trunk calls.
- voip-call-type—Specifies that the Stinger unit treats incoming calls as voice calls coming from the Public Switched Telephone Network (PSTN) for routing across a packet network bridge to another PSTN.
- phs-call-type—Specifies Personal Handyphone System (PHS) calls.
- v110-call-type—Specifies digital calls recognized as containing V.110 rate-adapted bearer channels.

**Example** `set call-route-type = trunk-call-type`

**Dependencies** Consider the following:

- The voip-call-type setting is supported only when voip-enabled is set to yes.
- When a Voice over IP (VoIP) software license has been enabled, the system creates a new call-route profile for each installed MultiDSP module that supports VoIP. The new call-route profile sets the call-route-type value to voip-call-type., which enables the system to route VoIP calls to the MultiDSP module.

When the unit receives a VoIP call on a network line, it routes the traffic internally on its time-division multiplexing (TDM) bus to the MultiDSP module, which handles VoIP-related functions such as audio coder/decoder (codec) processing, Real-Time Transport Protocol (RTP) processing, and UDP processing.

**Location** CALL-ROUTE

## call-routing-sort-method

**Description** Specifies whether to use the slot-first call-routing sort method or the item-first sort method for analog calls.

When the system resets, the Stinger unit creates the call-routing database by sorting the list of all installed devices. During active use, the Stinger unit resorts the list on the basis of system activity, but the initial sort order determines the initial order in which the unit uses host modules.

**Usage** Valid values are as follows:

- `item-first` (the default)—Specifies that the Stinger unit sorts by item number, then shelf, and then slot number. This setting tends to distribute incoming calls evenly across multiple host modules, resulting in load balancing across all modules, even after a system reset.
- `slot-first`—Specifies that the Stinger unit sorts by shelf and slot number, and then by item number. This setting tends to concentrate incoming calls on one host module at a time.

**Example** `set call-routing-sort-method = slot-first`

**Location** SYSTEM

## call-service

**Description** Read-only. Indicates the type of call service.

**Usage** Read-only parameter with one of the following values:

- `nailed-up`—This channel is not switched, but is permanent. No setup procedures are required.
- `switched`—The call is switched.
- `serial-wan`—The call is served by a serial WAN port or an xDSL port that acts like a serial WAN port.
- `atm-wan`—The call is connected to an E3-ATM, DS3-ATM, or OC3-ATM port.

**Example** `call-service = nailed-up`

**Location** `CALL-INFO`

## call-type

**Description** Specifies whether a session must remain established, even if inactive.

**Usage** Specify one of the following values:

- `off`—Enables the system to end inactive PPP over Ethernet (PPPoE) sessions and reestablish them when activity resumes.
- `ft1` (the default)—Keeps PPPoE sessions established indefinitely.
- `ft1-mpp`—*Not supported.*
- `ft1-bo`—*Not supported.*

**Example** `set call-type = off`

**Dependencies** This setting applies only to Stinger units that support PPPoE sessions to a router module.

**Location** `CONNECTION:telco-options`

## cap-equivalent-r-s

**Description** Read-only. Indicates the ring-to-shield equivalent capacitance in picofarads for copper loop test (CLT) module capacitance test.

**Usage** Read-only numeric value with a range of 0 to 4294967295.

**Example** `cap-equivalent-r-s = 1200`

**Location** `CLT-RESULT`

**cap-equivalent-t-r**

**Description** Read-only. Indicates the tip-to-ring equivalent capacitance in picofarads for copper loop test (CLT) module capacitance test.

**Usage** Read-only numeric value with a range of 0 to 4294967295.

**Example** `cap-equivalent-t-r = 1200`

**Location** CLT-RESULT

**cap-equivalent-t-s**

**Description** Read-only. Indicates the tip-to-shield equivalent capacitance in picofarads for copper loop test (CLT) module capacitance test.

**Usage** Read-only numeric value with a range of 0 to 4294967295.

**Example** `cap-equivalent-t-s = 1200`

**Location** CLT-RESULT

**carrier-established**

**Description** Read-only. Indicates whether error conditions exist on the physical line connection.

**Usage** Valid values for this read-only parameter are as follows:

- `true`—Indicates there are no error conditions.
- `false`—Indicates there are error conditions.

**Example** `carrier-established = false`

**Location** DS1-ATM-STAT  
T1-STAT

**cast-type**

**Description** Specifies the connection profile topology type.

**Usage** With the current software version, only the default value `p2p` (point-to-point) is valid.

**Example** `set cast-type = p2p`

**Location** CONNECTION:atm-options  
CONNECTION:atm-connect-options

## cbr

**Description** Specifies whether constant bit rate (CBR) traffic is enabled or disabled in this queue.

**Usage** Valid values are as follows:

- **yes**—Indicates the queue supports CBR traffic. This is the default.
- **no**—Indicates the queue does not support CBR traffic.

For each queue, one or more Asynchronous Transfer Mode (ATM) services categories can be set to **yes**. CBR must be set to **yes** for at least one and no more than two of the active queues assigned to a line interface module (LIM), control module, or trunk.

**Example** `set cbr = no`

**Location** SWITCH-CONFIG:atm-parameters:outgoing-queue

## cbsr-enable

**Description** Enables/disables the bootstrap router (BSR) router mechanism. When set to **yes**, the Stinger unit acts as a candidate BSR and takes part in electing a BSR in the Protocol Independent Multicast (PIM) domain. With the **yes** setting, you must specify a **cbsr-ip-address** value. This setting is not used when **enable** is set to **no**.

**Usage** Valid values are as follows:

- **yes**—Enables the BSR router mechanism.
- **no** (the default)—Disables the BSR router mechanism.

**Example** `set cbsr-enable = yes`

**Location** IP-GLOBAL:pim-options

## cbsr-interval

**Description** Number of seconds between transmission of bootstrap messages (BSMs). The default is to send BSMs every 60 seconds. This setting is not used when **cbsr-enable** is set to **no**.

**Usage** Specify a number of seconds from 5 to 900.

**Example** `set cbsr-interval = 120`

**Location** IP-GLOBAL:pim-options

### cbsr-ip-address

**Description** Local IP address the Stinger unit uses to send bootstrap messages (BSMs) when `cbsr-enable` is set to yes. This setting is not used when `cbsr-enable` is set to no.

**Usage** Specify an IP address in dotted decimal notation.

**Example** `set cbsr-ip-address = 1.1.1.101`

**Location** IP-GLOBAL:pim-options

### cbsr-priority

**Description** Bootstrap router (BSR) priority for the Stinger. The priority is used in the election of BSR. The system is more likely to be elected BSR with a higher priority value. To enable the system to exchange bootstrap messages (BSMs) without becoming BSR, leave the default zero setting, or set a low numeric value. This setting is not used when `cbsr-enable` is set to no.

**Usage** Specify a number from 0 (the default) to 255.

**Example** `set cbsr-priority = 1`

**Location** IP-GLOBAL:pim-options

### cdv-pm

**Description** Specifies a proportional multiplier (a percentage) used to determine significant change for the cell delay variation (CDV) metrics. CDV is a component of cell transfer delay (see `ctd-pm`), induced by buffering and cell scheduling and is associated with constant bit rate (CBR) and variable bit rate (VBR) quality of service (QoS).

**Usage** Specify a percentage. The default value is 25.

**Example** `set cdv-pm = 25`

**Location** PNMI-NODE-CONFIG[n]:node-timer

**See Also** `ctd-pm`

## cell-delay-variation-tolerance

**Description** Specifies the cell delay variation tolerance (CDVT) in microseconds.

**Usage** Specify a value in the range 0 (zero) to 1500 microseconds. The default value is 20. This setting is related to the *jitter* tolerance of the application. Use these guidelines to help you determine a setting:

- The ideal delay variation is 0 for an application such as voice.
- The default of 20 microseconds is a reasonable jitter threshold for most applications with a low tolerance for delay—for example, constant bit rate (CBR) and real-time variable bit rate (VBR) traffic applications.
- A higher value can be used for nonreal-time VBR and other applications that are not delay sensitive.

**Example** `set cell-delay-variation-tolerance = 50`

**Location** ATM-QOS

## cell-delineation

**Description** Read-only. Indicates that ATM cell delineation, which is cell transfer below the specified header error control (HEC) level, has been reached.

**Usage** Valid values for this read-only parameter are as follows:

- `true`—Indicates the receiver line has attained cell delineation. The physical line LED is turned on only after cell delineation has been reached.
- `false` (the default)—Indicates cell delineation has not been reached.

**Example** `cell-delineation = false`

**Location** DS1-ATM-STAT

## cell-level

**Description** *Not used.*

## cell-mode-first

**Description** *Not used.*

## cell-payload-scramble

**Description** Specifies whether cell payload scrambling in Asynchronous Transfer Mode (ATM) cells is enabled.

**Usage** Valid values are as follows:

- `yes`—Enables cell payload scrambling. This is the default.
- `no`—Disables cell payload scrambling

**Example** `set cell-payload-scramble = no`

**Location** DS3-ATM:line-config  
E3-ATM:line-config

## channel-mismatch-clear-timer-duration

**Description** Specifies the amount of time in tens of milliseconds allowed for clearing the timer in a channel mismatch in automatic protection switching (APS).

**Usage** Specify a number from 0 through 4,294,967,295. The default is 1000.

**Example** `set channel-mismatch-clear-timer-duration = 500`

**Location** APS-CONFIG

## channel-mismatch-failure

**Description** Read-only. Indicates whether one channel has been mistakenly matched with another.

**Usage** Valid values for this read-only parameter are as follows:

- `true`—A channel-mismatch failure has occurred.
- `false`—A channel-mismatch failure has not occurred.

**Example** `channel-mismatch-failure = false`

**Location** APS-STAT

## channel-mismatch-failure-timer-duration

**Description** Specifies the channel-mismatch failure timer duration in tens of milliseconds in automatic protection switching (APS).

**Usage** Specify a number from 0 through 4,294,967,295. The default is 250.

**Example** `set channel-mismatch-failure-timer-duration = 290`

**Location** APS-CONFIG



## channel-state

**Description** Read-only. Indicates the status of the physical connection on the line.

**Usage** Valid values for this read-only parameter are as follows:

- disabled—Indicates that line is configured as disabled.
- unavailable—Indicates that the line is enabled, but no customer premises equipment (CPE) device is connected to the IDSL port.
- nailed-up—Indicates that physical connection has been made.

**Example** channel-state = [ disabled disabled ]

**Location** IDSL-Stat  
T1-STAT

## channel-usage

**Description** *Not used.*

## chassis-serial-number

**Description** Read-only. Indicates the identity of the Stinger chassis.

**Usage** Read-only parameter with a range of 0 to 4294967295.

**Location** REDUNDANCY-STATS:context-stats:context-stats [n]

## check-far-end-ima-id

**Description** Enables or disables the verification of the far-end IMA ID during inverse multiplexing over ATM (IMA) group startup.

**Usage** Valid values are as follows:

- yes—Specifies that this check is enabled.
- no—Specifies that this check is not enabled. This is the default.

**Example** check-far-end-ima-id = no

**Location** IMAGROUP

## circuit-name

**Description** Indicates or specifies, according to the profile that includes it, the name of a circuit.

**Usage** Valid values for this parameter are as follows:

- In an atm-pvc-stat profile, circuit-name is a read-only value for the name of the permanent virtual circuit (PVC).
- In an atm-vcc-stat profile, circuit-name is a read-only value for the name of the virtual channel connection (VCC).
- In the fr-options subprofile of a connection profile, you can specify a name for the peer frame relay data link for a frame relay circuit, using up to 14 characters.



**Note** If you are configuring IDSL, and you do not specify circuit-name in the fr-options subprofile of the connection profile, the Stinger unit automatically creates a circuit name based on the vpi, vci, and nailed-group parameters set in the atm-connect-options subprofile.

- In frdlci-stat and frpvc-stat profiles, the circuit name is a read-only parameter containing the name of the peer frame relay data link.

**Example** set circuit-name = ozone1

**Location** ATMPVC-STAT  
 ATMVCC-STAT  
 CONNECTION:fr-options  
 FRDLCI-STAT  
 FRPVC-STAT

## clear-call

**Description** *Not used.*

**Location** TERMINAL-SERVER:terminal-mode-configuration

## clear-screen

**Description** *Not used.*

**Location** TERMINAL-SERVER:terminal-mode-configuration

## clid

**Description** Specifies the calling line number for authentication.

**Usage** Specify an alphanumeric value of up to 24 characters. The default value is blank.

**Example** set clid = 510-555-1212

**Location** CONNECTION

## clid-auth-mode

**Description** *Not supported.* Specifies an authentication mode to occur before the system retrieves a caller's profile by using the caller ID or called number.

**Location** ANSWER-DEFAULTS  
CONNECTION:answer-options

## clid-selection

**Description** *Not supported.* Specifies whether to use a Public Switched Telephone Network (PSTN) caller ID or one supplied by the device requesting a session.

**Location** ANSWER-DEFAULTS  
CONNECTION:tunnel-options

## client-auth-id

**Description** Specifies the Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) system name used for tunnel authentication. The name is sent to the L2TP network server (LNS) in Start Control Connection Request (SCCRQ) packets.

Tunnel authentication can be configured on a tunnel server end point level or on a connection basis. It occurs during tunnel establishment.

**Usage** Specify the LAC name, up to 31 characters. The default is null.

**Example** `set client-auth-id = nyserver`

**Location** CONNECTION:tunnel-options  
TUNNEL-SERVER

## client-default-gateway

**Description** Specifies a default gateway for traffic from this connection if no specific route appears in the IP routing table.

**Usage** Specify an IP address. The default is 0.0.0.0, which causes the system to use the default route.

**Example** `set client-default-gateway = 2.2.2.2`

**Location** CONNECTION:ip-options

## client-dns-addr-assign

**Description** Enables or disables client Domain Name System (DNS) for the connection. When client DNS is enabled, the system presents client DNS server addresses while negotiating the connection. The addresses it presents can be specified in the connection profile or ip-global profile.

**Usage** Valid values are as follows:

- **yes**—Makes the client DNS server addresses available to the connection. This is the default.
- **no**—Does not make the client DNS server addresses available.

**Example** `set client-dns-addr-assign = no`

**Location** `CONNECTION:ip-options`

## `client-dns-primary-addr`

**Description** Specifies the IP address of a client Domain Name System (DNS) server for the connection. Client DNS servers provide a way to protect your local DNS information from WAN users. Client DNS has two levels: a global configuration, and a connection-specific configuration. This setting applies to the connection-specific level.

**Usage** Specify the IP address of the primary DNS server for the connection. The default is 0.0.0.0/0, which specifies that no primary DNS server is available for the connection.

**Example** `set client-dns-primary-addr = 3.3.3.3/28`

### **Dependencies**

- If `client-dns-addr-assign` is set to `no`, this setting does not apply.
- If this setting is null, and client DNS has been configured system-wide in the `ip-global` profile, the system uses the global client DNS server address.

**Location** `CONNECTION:ip-options`

## `client-dns-secondary-addr`

**Description** Specifies the IP address of a secondary client Domain Name System (DNS) server for the connection. The unit presents this server address during IP Control Protocol (IPCP) negotiation only if the server specified by `client-dns-primary-addr` is inaccessible.

**Usage** Specify the IP address of the secondary DNS server for the connection. The default is 0.0.0.0/0, which specifies that no secondary DNS server is available for the connection.

**Example** `set client-dns-secondary-addr = 4.4.4.4/28`

**Dependencies** If `client-dns-addr-assign` is set to `no`, this setting does not apply.

**Location** `CONNECTION:ip-options`

## client-primary-dns-server

**Description** Specifies the IP address of the primary client Domain Name System (DNS) server for remote customer premises equipment (CPE) devices that do not have a client DNS server defined in the client's profile. The address is presented to WAN connections during IP Control Protocol (IPCP) negotiation.

Client DNS can be specified system-wide to allow all CPE to access one or two DNS servers. Or it can be configured on a connection basis, to allow each appropriately configured connection to access one or two specific servers. At the system level, client DNS also allows an exit mechanism to the local servers if the client servers are inaccessible.

When specified in a `vrouter` profile, the effect of this DNS setting is similar to that in the `ip-global` profile, but is exclusive to the virtual router. If DNS settings are not specified in a `vrouter` profile, the virtual router uses the DNS settings defined in the `ip-global` profile

**Usage** Specify the IP address of a DNS server for CPE devices that do not require a connection-specific client DNS configuration. The default is `0.0.0.0/0`, which specifies that no client DNS server is available on a global level.

**Example** `set client-primary-dns-server = 1.1.1.1/28`

**Location** IP-GLOBAL  
VROUTER

## client-secondary-dns-server

**Description** Specifies the IP address of a secondary client Domain Name System (DNS) server for remote customer premises equipment (CPE) devices that do not have a client DNS server defined in the client's profile. The address is presented to WAN connections during IP Control Protocol (IPCP) negotiation.

Client DNS can be specified system-wide to allow all CPE to access one or two DNS servers. Or it can be configured on a connection basis, to allow each appropriately configured connection to access one or two specific servers. At the system level, client DNS also allows an exit mechanism to the local servers if the client servers are inaccessible.

When specified in a `vrouter` profile, the effect of this DNS setting is similar to that in the `ip-global` profile, but is exclusive to the virtual router. If DNS settings are not specified in a `vrouter` profile, the virtual router uses the DNS settings defined in the `ip-global` profile

**Usage** Specify the IP address of a DNS server for CPE devices that do not require a connection-specific client DNS configuration. The default is `0.0.0.0/0`, which specifies that no client DNS server is available on a global level.

**Example** `set client-secondary-dns-server = 2.2.2.2/28`

**Location** IP-GLOBAL  
VROUTER

## client-wins-addr-assign

**Description** Enables or disables client Windows Internet Name Service (WINS) for the connection. When client WINS is enabled, the system presents client WINS server addresses while negotiating the connection. The addresses it presents can be specified in the `connection` profile or `ip-global` profile.

**Usage** Valid values are as follows:

- `yes`—Makes the client WINS server addresses available to the connection. This is the default.
- `no`—Does not make the client WINS server addresses available.

**Example** `set client-wins-addr-assign = no`

**Location** `CONNECTION:ip-options`

## client-wins-primary-addr

**Description** Specifies the IP address of a client Windows Internet Name Service (WINS) server for the connection.

Client WINS servers provide a way to protect your local WINS information from WAN users. Client WINS has two levels: a global configuration that applies to all PPP connections, and a connection-specific configuration. This setting applies to the connection-specific level.

The system uses the global client addresses only if the `connection` profile specifies no WINS server addresses. You can also choose to present your local WINS servers to clients if no other servers are defined or available.

**Usage** Specify the IP address of the primary WINS server for the connection. The default is `0.0.0.0/0`, which specifies that no primary WINS server is available for the connection.

**Example** `set client-wins-primary-addr = 3.3.3.3/28`

**Dependencies** If `client-wins-addr-assign` is set to `no`, this setting does not apply.

**Location** `CONNECTION:ip-options`

## client-wins-secondary-addr

**Description** Specifies the IP address of a secondary client Windows Internet Name Service (WINS) server for the connection. The unit presents this server address during IP Control Protocol (IPCP) negotiation only if the server specified by `client-wins-primary-addr` is inaccessible.

**Usage** Specify the IP address of the secondary WINS server for the connection. The default is `0.0.0.0/0`, which specifies that no secondary WINS server is available for the connection.

**Example** `set client-wins-secondary-addr = 4.4.4.4/28`

**Dependencies** If `client-wins-addr-assign` is set to `no`, this setting does not apply.

**Location** `CONNECTION:ip-options`

## cli-user-auth

**Description** Specifies whether the Stinger unit authenticates a command-line-interface user by means of local profiles or an external authentication server, and if the authentication is to be in any specific order.

**Usage** Specify one of the following settings:

- `local-then-external`—Specifies that the Stinger unit uses local user profiles for the first authentication attempt. If that attempt fails, the unit attempts authentication through an external server, if an external authentication server exists. This is the default.
- `local-only`—Specifies that the Stinger unit uses only local user profiles.
- `external-only`—Specifies that the Stinger unit uses only an external authentication server and ignores local user profiles.
- `external-then-local`—Specifies that the Stinger unit authenticates by means of an external authentication server. If authentication fails or times out, the unit uses local user profiles to make another attempt.
- `external-then-local-if-timeout`—Specifies that the Stinger unit authenticates by means of an external authentication server. If authentication times out, the unit uses local user profiles to make another attempt.

**Example** `set cli-user-auth = local-only`

**Location** `EXTERNAL-AUTH`

## clock-change-trap-enabled

**Description** Enables or disables the system generation of a trap (notification) on a clock change.

**Usage** Select one of the following values:

- `yes`—Clock change generates a trap.
- `no`—Clock change does not generate a trap. This is the default.

**Example** `set clock-change-trap-enabled = yes`

**Location** `TRAP`

## clock-priority

**Description** Assigns a clock source priority to an interface.

When multiple interfaces are eligible to be the clock source for synchronous transmissions, the Stinger unit uses the value you specify to select an interface as the master clock source.

**Usage** Valid values are as follows. The default is middle-priority in all profiles except ds1-atm, in which the default is high-priority.

- **high-priority**—Specifies the highest priority. The Stinger unit chooses an interface with this priority setting as the clock source over other interfaces with a lower priority. If more than one interface has the highest priority, the first available interface becomes the clock source.
- **middle-priority**—Specifies the second priority. The Stinger unit chooses an interface with this priority setting if every interface with a high-priority setting is unavailable. If more than one interface has a middle-priority setting, the first available middle-priority interface becomes the clock source.
- **low-priority**—Specifies the lowest priority. The Stinger unit chooses an interface with this priority only if every interface with a higher priority setting is unavailable. If more than one interface has a low-priority setting, the first available low-priority interface becomes the clock source.

Once the Stinger unit chooses an interface as the clock source, it uses that interface until it becomes unavailable, or a until a higher-priority source becomes available.

**Example** set clock-priority = middle-priority

**Dependencies** Consider the following:

- If clock-source is set to not-eligible, this setting does not apply.
- If multiple interfaces are eligible to be the clock source and each interface has an equal clock-priority value, the Stinger unit chooses a clock source at random.

**Location** DS1-ATM:line-config

DS3-ATM:line-config

E3-ATM:line-config

OC3-ATM:line-config

HDSDL2:line-config

SHDSL:line-config

## clock-source

**Description** Specifies whether a Stinger unit can use an interface as the master clock source for its timing subsystem.

**Usage** Valid values are as follows:

- **eligible**—The system can obtain its clock signal from the port.
- **not-eligible** (the default)—The system cannot use the port for a clock source.

**Example** set clock-source = eligible

**Location** DS1-ATM:line-config

DS3-ATM:line-config

E3-ATM:line-config

OC3-ATM:line-config

HDSDL2:line-config

SHDSL:line-config



## cltm-shelf

**Description** Identifies the shelf where a copper loop test (CLT) is to be performed. The system uses a value of 1 for a standalone or host unit or the shelf number of a remote unit as the index in the CLT-MS-ACCES profile.

**Usage** Enter the shelf number, preceded by shelf-.

**Example** set cltm-shelf = shelf-2

**Location** CLT-MS-ACCESS

## cltm-slot

**Description** Specifies the number of the slot in which a copper loop test (CLT) module or path selector module (PSM) is installed.

**Usage** Enter the slot number, preceded by slot-.

**Example** set cltm-slot = slot-15

**Location** CLT-MS-ACCESS

CLT-COMMAND

CLT-RESULT

## clt-slot-number

**Description** Read-only. Indicates the number of the slot in which a copper loop test (CLT) module or path selector module (PSM) is installed.

**Usage** The clt-slot-number value is read-only.

**Example** clt-slot-number = any-slot

**Location** LINE-TESTS

## code-violations

**Description** Read-only. Indicates the number of cyclic redundancy check (CRC) anomalies occurring during the accumulation period. Use this parameter to check interface operations.

**Usage** The code-violations value is read-only.

**Example** code-violations = 17

**Location** AL-DMT-STAT:physical-statistic

HDLSL2-STAT:physical-statistic

SDSL-STAT:physical-statistic

SHDSL-STAT:physical-statistic

**coil-detection-coil-count**

**Description** Read-only. Indicates the number of load coils detected during a copper loop test (CLT).

**Usage** The coil-detection-coil-count value is read-only.

**Example** coil-detection-coil-count = 2

**Location** CLT-RESULT

**coldstart-enabled**

**Description** Specifies whether the system generates a notification (trap) when the Stinger unit reinitializes itself so that the configuration of the SNMP manager or the system itself might be altered.

**Usage** Valid values are as follows:

- **yes**—Specifies that the system generates a trap when the Stinger unit reinitializes itself so that the configuration of the SNMP manager or the system itself might be altered. This is the default.
- **no**—Specifies that the system does not generate a notification (trap) when the Stinger unit reinitializes itself so that the configuration of the SNMP manager or the system itself might be altered.

**Example** set coldstart-enabled = no

**Location** TRAP

**command [n]**

**Description** Commands to allow or exclude.

**Usage** Specify up to 512 commands that the users are allowed to use or are excluded from using.

**Example** set command 1 = write

**Dependencies** This parameter is used in conjunction with the exclude-listed-commands parameter.

**Location** USER-GROUP

## community-minus-1

**Description** *Not used.* Specifies a number representing the highest level of the Private Network-to-Network Interface (PNNI) hierarchy that lies within the community minus one scope.

**Usage** Specify a number from 1 (one) to 104. The default is 64.

**Example** `set community-minus-1 = 64`

**Location** PNNI-NODE-CONFIG:node-scope-mapping

## community-name

**Description** Specifies the SNMP community name associated with SNMP protocol data units (PDUs). The string you specify becomes a password that the Stinger unit sends to the SNMP manager when an SNMP notification (trap) event occurs. The password authenticates the sender identified by `host-address`.

**Usage** Specify a community name of up to 31 characters. The default is `public`.

**Example** `set community-name = mycomm`

**Location** TRAP

## community-plus-1

**Description** *Not used.* Specifies a number representing the highest level of the Private Network-to-Network Interface (PNNI) hierarchy that lies within the community plus one scope.

**Usage** Specify a number from 1 (one) to 104. The default is 48.

**Example** `set community-plus-1 = 48`

**Location** PNNI-NODE-CONFIG[n]:node-scope-mapping

## comp-neq

**Description** Specifies whether to test for packet data that is equal to a specified value or not equal to that value.

**Usage** Valid values are as follows:

- `yes`—The comparison succeeds (the filter matches) if the contents do not equal the specified value.
- `no` (the default)—The comparison succeeds when the values are equal. For a filter that requires the packet contents to equal the specified value, leave `comp-neq` (*compare-not-equals*) set to `no`.

**Example** `set comp-neq = no`

**Dependencies** This setting applies only if the type parameter in the input-filter or output-filter subprofile is set to generic-filter.

**Location** FILTER:input-filters[n]:gen-filter  
FILTER:output-filters[n]:gen-filter

## config-change-enabled

**Description** Specifies whether the Stinger unit generates a Simple Network Management Protocol (SNMP) Config-Change notification (trap 30) whenever the system configuration is modified or a new software version is loaded.

**Usage** Valid values are as follows:

- yes (the default)—Specifies that the trap is enabled.
- no—Specifies that the trap is not enabled.

**Example** set config-change-enabled = no

**Location** TRAP

## config-side

**Description** Specifies the role of the managed entity as one side of the Asynchronous Transfer Mode (ATM) interface.

**Usage** Valid values are as follows:

- user—The managed entity has the role of user.
- network—The managed entity has the role of network.
- other—This is the default.

**Example** set config-side = other

**Dependencies** This value does not apply when config-type is set to atmf-pnni1dot0.

**Location** ATM-IF-CONFIG:extension-config

## config-type

**Description** Specifies the type of connection setup procedures configured for the ATM interface.

**Usage** Specify one of the following values:

- atmf-uni-pvc-only (the default)
- atmf-pnni1dot0—For trunk port interfaces, this value enables a Private Network-to-Network Interface (PNNI) setup.
- atmf-auto-config—Sets the configuration type automatically.

**Example** set config-type = atmf-pnni1dot0

**Location** ATM-IF-CONFIG:extension-config

## connection-profile-auto-naming-convention

**Description** Specifies the naming convention for connection profiles generated by the system when a cross-connect entry has been created via SNMP.

**Usage** Valid values are as follows:

- lower-interface-number-first (the default)—Creates a connection profile and assign 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. For example:

```
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
```

- atm-options-entry-first—Creates a connection profile and assign 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).

```
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
```

**Example** set connection-profile-auto-naming-convention =  
atm-options-entry-first

**Location** SYSTEM

## conn-estab-interval

**Description** Specifies the number of seconds between successive transmissions of interim link management interface (ILMI) messages on this interface for the purpose of detecting establishment of ILMI connectivity. *ILMI is not supported with the current software version.*

**Usage** Set a value from 1 to 65535 seconds. The default value is 1 (one).

**Example** set conn-estab-interval = 15

**Location** ATM-IF-CONFIG:extension-config

## conn-kind

**Description** Specifies the kind of soft permanent virtual circuit (SPVC).

**Usage** With the current software version, valid values are as follows:

- `pvc`—Specifies a virtual link of a permanent virtual circuit (PVC)/permanent virtual path (PVP). This is the default.
- `spvc-initiator`—Specifies a virtual link at the permanent virtual channel (PVC) side of an SPVC—the line interface module (LIM)-side connection to customer premises equipment (CPE).
- `spvc-target`—Specifies a virtual link at the PVC side of an SPVC where the switch is the target of the SPVC setup
- `svc-incoming`—*Not used*. Specifies a virtual link established after reception of a signaling request to set up a switched virtual connection (SVC).
- `svc-outgoing`—*Not used*. Specifies a virtual link established after forwarding or transmission of a signaling request to set up an SVC.



**Note** With the current software version, the settings specified by `svc-incoming` and `svc-outgoing` are build dynamically by the system and are unavailable in the TAOS command-line interface.

**Example** `set conn-kind = spvc-target`

**Location** `CONNECTION:atm-connect-options`  
`CONNECTION:atm-options`

## conn-user

**Description** Read-only. Indicates whether a soft permanent virtual circuit (SPVC) connection is for a user or for a signaling channel.

**Usage** Valid values for this read-only parameter are as follows:

- `default`—Represents any normal user connection.
- `cpes` (common part convergence sublayer)—Indicates that the profile was created automatically for use by the ATM signaling control channel.

**Example** `conn-user = default`

**Location** `CONNECTION`

## console-enabled

**Description** Specifies whether the system generates an SNMP notification (trap) when the console has changed state.

**Usage** Valid values are as follows:

- **yes**—Specifies that the system generates a trap when the console has changed state. This is the default.
- **no**—Specifies that the system does not generate a trap when the console has changed state.

**Example** `set console-enabled = no`

**Location** TRAP

## console-mode

**Description** Specifies the console mode used on the serial console (diagnostic) port.

**Usage** Valid values are as follows:

- **on** (the default)—Specifies that the console port is activated for the specified control module.
- **off**—Specifies that the console port is not activated for the specified control module.
- **y-cable**—Specifies that the console port on a unit with redundant control modules uses automatic mode. In this mode, when control of the system switches to the secondary control module so that the secondary became primary, that control module's console also switches over and becomes active. This is a kind of console redundancy.

**Example** `set console-mode = y-cable`

**Dependencies** For the **y-cable** setting to apply, the serial ports of both redundant control modules must be connected through a Y-cable to an administrative terminal.

**Location** SERIAL

## contact

**Description** Specifies the person or department to contact for reporting error conditions. The contact value is SNMP readable and settable.

**Usage** Specify the name of a contact person or department. You can enter up to 80 characters. The default is null.

**Example** `set contact = rchu`

**Location** SNMP

#### contact-closure [n]

**Description** An array of indexed parameters that indicate the contact closure state on the corresponding remote shelf.



**Note** Only the first two contact closure values are meaningful for Stinger MRT units.

**Usage** This parameter is read-only. Valid values are as follows:

- yes—Contact-closure sensors on the remote shelf indicate loss of contact closure.
- no (the default)—Contact-closure sensors on the remote shelf indicate closure.

**Example** `contact-closure[1] = no`

**Location** `REMOTE-SHELF-STAT`

#### context-prefix

**Description** Specifies a name to be compared with the name present in the incoming or outgoing protocol data unit (PDU), either as a prefix or as a complete match. This parameter must be configured as part of the view based access control model (VACM).

**Usage** Specify a name in plain text of up to 32 characters.

**Example** `set context-name = electra`

**Dependencies** The value of `match-method` determines how the value of `context-prefix` is matched in the incoming or outgoing PDU:

- If `match-method` is set to `exact-match`, the name in the PDU must match exactly.
- If `match-method` is set to `prefix-match`, only the prefix of the name in the PDU must match.

**Location** `VACM-ACCESS:access-properties`

#### continuity-level

**Description** Specifies the type of continuity test.

**Usage** Specify one of the following values:

- `end-to-end`—Specifies testing at the end-to-end level.
- `segment` (the default)—Specifies testing at the segment level.

**Example** `set continuity-level = end-to-end`

**Location** `ATM-OAM:continuity-config`



## contract-name

**Description** Specifies a name in one of two profiles:

- In an atm-qos profile, contract-name specifies the unique name of the quality-of-service (QoS) contract used with one or more Asynchronous Transfer Mode (ATM) connections.
- In an atm-prefix profile, contract-name specifies the name of the profile.

**Usage** Valid values are as follows:

- In an atm-qos profile, specify a text string of up to 16 characters. The default is null.
- In an atm-prefix profile, specify a name of up to 20 characters. The name specifies the profile with the default index containing the system-generated ATM prefix.

**Dependencies** In the atm-qos profile only, if encapsulation-protocol is not set to atm or atm-circuit, contract-name does not apply.

### Example

- For an atm-qos profile:  
set contract-name = contract002
- For an atm-prefix profile:  
set contract-name = target-2

**Location** ATM-PREFIX  
ATM-QOS

## control-bus-type

**Description** Specifies how to send control bus messages.

**Usage** Valid values are as follows:

- dpram (dual port RAM; the default)—Specifies a single shared bus between the control module and each line interface module (LIM). It is an extension of the control module processor.
- pbus (packet bus)—Specifies an ATM start connection between the control module and each LIM.

**Example** set control-bus-type = pbus

**Location** SYSTEM

## control-connect-establish-timer

**Description** Specifies the number of seconds during which the system can establish a Layer 2 Tunneling Protocol (L2TP) tunnel with another host. Any change you make to this value takes effect when the previous timer expires.

**Usage** Specify a number from 0 to 600. The default is 60.

**Example** set control-connect-establish-timer = 120

**Location** L2-TUNNEL-GLOBAL:l2tp-config

## controller-switchover-enabled

**Description** Enables or disables system generation of a trap (notification) on a control module switchover in a redundant system.

**Usage** Select one of the following values:

- yes—Control module change generates a trap.
- no—Control module change does not generate a trap.

**Example** set controller-switchover-enabled = yes

**Location** TRAP

## core-dump-rip-update

**Description** Specifies the RIP update rate during a core dump.

**Usage** Specify one of the following values:

- update-higher-freq—RIP updates are sent in higher frequency during core dumps.
- update-high-freq (the default)—RIP updates are sent in high frequency during core dumps.
- update-med-freq—RIP updates are sent in medium frequency during core dumps.
- update-low-freq—RIP updates are sent in low frequency during core dumps.
- update-lower-freq—RIP updates are sent in lower frequency during core dumps.
- update-off—RIP updates are not sent during core dumps.

**Example** set core-dump-rip-update = update-off

**Location** DEBUG

## corrected-hec-error-count

**Description** Read-only. Number of corrected header check sequence (HCS) errors since the Stinger unit was last reset.

**Usage** The corrected-hec-error-count value is read-only.

**Example** corrected-hec-error-count = 0

**Location** DS3-ATM-STAT  
E3-ATM-STAT  
OC3-ATM-STAT

## correction-factor

**Description** Specifies the number of failures that must be detected by control module self-tests before a correction is made. The system is configured by default to perform background integrity tests of the control module application-specific integrated circuit (ASIC) at a specified interval (10 milliseconds by default).

**Usage** Valid values range from 1 (one) through 20. The default is 5.

The system keeps a history of the past 20 tests. If the correction factor is 1, 1 failure out of the past 20 tests results in a correction. If the correction factor is 5, 5 failures out of 20 result in a correction.

**Example** set correction-factor = 6

**Location** SYSTEM-INTEGRITY:integrity-config

## coset-enabled

**Description** *Not used.* Specifies whether the ATM Forum polynomial (coset polynomial) is added to the header error control (HEC) field, in the transmit direction, before the HEC verification of a received cell.

**Usage** Specify one of the following values:

- yes (the default)—Specifies that the ATM Forum coset polynomial value is added to HEC before the HEC verification of a received cell.
- no—Specifies that the ATM Forum polynomial (coset polynomial) is not added to HEC before the HEC verification of a received cell.

**Example** set coset-enabled = no

**Location** DS1-ATM:line-config

## cost

**Description** Cost of an OSPF link. The lower the cost, the more likely OSPF is to use the interface to forward data traffic.

The value you can enter for `cost` depends upon your configuration:

**Usage** Specify a number from 1 through 16777214. The default is 1 on the Ethernet interface, or 10 on a WAN link. With the exception of links to stub networks, the output cost must always be nonzero. A link with a cost of 0xFFFFF (16777215) is considered nonoperational.

**Example** `set cost = 50`

**Dependencies** In a static route, interpretation of the `cost` value depends on the type of external metric set by `ase-type`. If the Stinger unit is advertising type 1 metrics, OSPF can use the specified number as the cost of the route. Type 2 external metrics are an order of magnitude larger. Any type 2 metric is considered greater than the cost of any path internal to the autonomous system.

**Location** CONNECTION:ip-options:ospf-options,  
IP-INTERFACE:ospf

## countries-enabled

**Description** Read-only. Indicates the bit set identifying the countries enabled in the Stinger unit.

**Usage** The `countries-enabled` setting is read-only.

**Example** `countries-enabled = 511`

**Location** BASE

## country-code

**Description** Specifies the country location regarding modem settings, to program the modem for any operational parameters that need to be adjusted for national regulations or telephone networks.

**Usage** Valid values are as follows. The default value is `unitedstates`.

|             |            |          |             |
|-------------|------------|----------|-------------|
| australia   | austria    | belgium  | brazil      |
| bulgaria    | canada     | china    | czechslovak |
| denmark     | finland    | france   | germany     |
| greece      | hongkong   | hungary  | india       |
| ireland     | israel     | italy    | japan       |
| korea       | luxembourg | malaysia | mexico      |
| netherlands | newzealand | norway   | philippines |
| poland      | portugal   | ruissia  | singapore   |
| southafrica | spain      | sweden   | switzerland |

taiwan                      unitedkingdom                      unitedstates

**Example** set country-code = malaysia

**Dependencies** When the modem profile is updated and written, a check is made to see if the modem supports the selected value for country-code. If the modem supports the value, it is programmed with the new country code. If the modem does not support the selected country code then country-code is not updated with the new value and an error message is logged.

**Location** MODEM

## cp-bit-error-count

**Description** Read-only. Indicates the number of parity errors on C-bit-parity lines since the last time the unit was reset.

**Usage** The cp-bit-error-count value is read-only.

**Example** cp-bit-error-count = 0

**Location** DS3-ATM-STAT  
E3-ATM-STAT

## cross-connect-index

**Description** Read-only. Indicates the cross-connect index in the AToM MIB. A cross-connect receives a cell stream on one interface and transmits it on another.

**Usage** The cross-connect-index value is read-only.

**Example** cross-connect-index = 0

**Location** CONNECTION

## cslip-auto-detect

**Description** *Not used.*

## ctd-pm

**Description** Specifies the proportional multiplier (a percentage) used to determine significant change for the cell transfer delay (CTD) metrics. Cell transfer delay is the elapsed time between a cell exit event at one interface for a connection, such as the source User-Network Interface (UNI), and the corresponding cell entry event at another interface, such as the destination UNI. The cell transfer delay between two measurement points is the sum of the total inter-ATM node transmission delay.

**Usage** Specify a percentage from 1 to 99. The default is 50.

**Example** set ctd-pm = 60

**Location** PNNI-NODE-CONFIG[n]:node-timer

## ctone-tone

**Description** Specifies the type of control tone to be used in a copper loop test (CLT).

**Usage** Valid values are as follows:

- quiet—Specifies the quiet type of tone. This is the default.
- restore—Specifies that a normal tone type is restored.

**Example** `set ctone-tone = restore`

**Location** CLT-COMMAND

## ctone-type

**Description** Specifies the type of DSL service to use for the control tone in a copper loop test (CLT).

**Usage** Valid values are as follows:

- adsl—Specifies that ADSL is used for the control tone. This is the default.
- glite—Specifies that G.lite is used for the control tone.

**Example** `set ctone-typt = glite`

**Location** CLT-COMMAND

## current-state

**Description** Read-only. Indicates the state of a slot, a permanent virtual circuit (PVC), or an ATM virtual channel connection (VCC), depending on the profile.

**Usage** Valid values for this read-only parameter are as follows:

- In a slot-state profile, `current-state` indicates the current operational state of the slot and can have one of the following values:
  - `oper-state-down`—The slot is in a nonoperational state.
  - `oper-state-up`—The slot is in normal operations mode.
  - `oper-state-diag`—The slot is in diagnostics mode.
  - `oper-state-dump`—The slot is dumping its memory.
  - `oper-state-pend`—The slot is no longer down, but is not yet ready for normal operation. This value denotes a transitional state in which additional shelf-to-slot communications are required to make the slot fully operational.
  - `oper-state-post`—The slot is running a self-test.
  - `oper-state-maint`—This state indicates the operator explicitly took the card out of operation.
  - `oper-state-none`—The slot is empty.
- In an `atmpvc-stat` profile, `current-state` indicates the current state of the ATM permanent virtual circuit (PVC) and can have one of the following values:
  - `pvc-inactive`—The PVC is inactive.
  - `pvc-closed`—The PVC exists, but it is closed.
  - `pvc-data-transfer`—The PVC is active, and data can be transferred.
- In an `atmvcc-stat` profile, `current-state` indicates the current state of the ATM virtual channel connection (VCC) and can have one of the following values:
  - `vcc-inactive`—The VCC is inactive.
  - `vcc-closed`—The VCC exists, but it is closed.
  - `vcc-data-transfer`—The VCC is active, and data can be transferred.
- In an `frpvc-stat` or `frdlci-stat` FRPVC-STAT or FRDLCI-STAT profile, `current-state` indicates the current state of the permanent virtual circuit (PVC) and can have one of the following values:
  - `pvc-inactive`—The PVC is inactive.
  - `pvc-closed`—The PVC exists, but it is closed.
  - `pvc-data-transfer`—The PVC is active, and data can be transferred.

**Example** `current-state = pvc-inactive`

**Location** `ATMPVC-STAT`  
`ATMVCC-STAT`  
`FRDLCI-STAT`  
`FRPVC-STAT`  
`SLOT-STATE`

## `curr-node-id`

**Description** Specifies the value that the unit is currently using to represent itself as this Private Network-to-Network Interface (PNNI) node.

**Usage** Specify either the PNNI node ID generated by the system or the ID manually entered for `node-id`.

**Example** `set curr-node-id =`  
`48:a0:39:84:0f:80:01:bc:72:00:01:d0:6a:96:00:ff:d0:6a:+`

**Location** PNNI-NODE-CONFIG

## `curr-node-peer-group-id`

**Description** Specifies the value the unit is currently using as its peer group ID.

**Usage** Specify either the Private Network-to-Network Interface (PNNI) peer group ID generated by the system, or the ID manually entered in `node-peer-group-id`.

**Example** `set curr-node-peer-group-id =`  
`48:39:84:0f:80:01:bc:72:00:01:00:00:00:00:00`

**Location** PNNI-NODE-CONFIG



---

## D

### `dadsl-atm-24`

**Description** Specifies whether code images for ADSL 24-port line interface modules (LIMs) are to be stored in flash memory.

**Usage** Valid values are as follows:

- `auto`—Specifies that the system loads the code image if an ADSL 24-port LIM is installed. This is the default.
- `load`—Specifies that the system loads the code image when one is present in the tar file.
- `skip`—Specifies that the system skips the code image when one is present in the tar file.



**Note** A module is considered present in the system if a `slot-type` profile exists for that module type. The system creates a `slot-type` profile when it first detects the presence of a module, and does not delete the profile unless you use the `slot -r` command to permanently remove a module that is no longer installed in the system, or clear nonvolatile RAM (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.

**Example** `set dadsl-atm-24 = auto`

**Location** `LOAD-SELECT`

### `data-call-enabled`

**Description** Read-only. Indicates whether the Stinger unit supports data calls over integrated services digital network (ISDN) lines.

**Usage** The `data-call-enabled` parameter setting is read-only. Valid values are as follows:

- `yes`—Indicates that the Stinger unit supports data calls over ISDN lines.
- `no` (the default)—Indicates that the Stinger unit does not support data calls over ISDN lines.

**Example** `data-call-enabled = yes`

**Location** `BASE`

## data-filter

**Description** Specifies the name of a filter to apply to the interface. The filter name can be from a local filter profile or RADIUS pseudo-user profile.

The setting in the `answer-defaults` profile is used only for RADIUS-authenticated connections that do not specify a data filter.

If the system applies both a call filter and a data filter to a connection, it applies the data filter first. Only those packets that the data filter forwards reach the call filter.

**Usage** Specify the filter name. The default is null, which indicates no filter.

**Example** `set data-filter = ip-spoof`

**Dependencies** If a local connection profile does not use authentication, it cannot specify a RADIUS filter profile. *Filters are not supported with the current software version.*

**Location** `ANSWER-DEFAULTS:session-info`  
`CONNECTION:session-options`

## data-ip-address

**Description** Specifies the IP address of the Ethernet port to be used for stacking data traffic. The system advertises the address to other members of the stack in stacking control packets, and those systems, in turn, send stacking data packets to the address you specify.

**Usage** Specify an IP address in dotted decimal notation. The default is 0.0.0.0, which specifies that the `system-ip-addr` value is advertised instead of the `data-ip-address` value.

**Example** `set data-ip-address = 1.1.1.1`

**Dependencies** The Stinger unit supports a soft IP interface, which is an internal interface that is always operational. Routing protocols always advertise the soft interface address as reachable on all interfaces that are operational and running a routing protocol. Like the `system-ip-addr`, the `data-ip-address` is an area of memory that contains the address of one of the Ethernet interfaces of the Stinger unit.

If the specified interface becomes unavailable, all stacking data packets destined for the interface are lost. Some applications use the soft interface for the `data-ip-address` value to keep from being bound to a particular interface. To use the soft interface as the destination for stacking data packets, enter the soft IP interface address for `data-ip-address`.

**Location** `STACKING`

## data-rate-mode

**Description** Specifies the per-session DSL data-rate mode.

**Usage** Valid values are as follows:

- **autobaud**—Specifies that a DSL modem must train up to a set data rate. If a DSL modem cannot train to this data rate, it connects at the closest rate to which it can train (the modem's ceiling rate).
- **singlebaud** (the default)—Specifies that the device trains to a single data rate, even if the DSL modem can train at a higher or lower data rate.



**Note** Currently, only the **singlebaud** setting is supported on the SDSL module.

**Example** `set data-rate-mode = singlebaud`

**Location** `SDSL:line-config`

## data-service

**Description** *Not supported.* Specifies the type of service requested of a telephone company central office (CO) switch.

**Location** `CONNECTION:telco-options`

## dc-delta-resistance-r-s

**Description** Read-only. Indicates the ring-to-shield resistance in ohms for a copper loop test (CLT) module dc-delta resistance test.

**Usage** Read-only numeric field with a range of 0 to 4294967295. The value 99999999 indicates that the measurement is over range.

**Example** `dc-delta-resistance-r-s = 1200`

**Location** `CLT-RESULT`

## dc-delta-resistance-t-r

**Description** Read-only. Indicates the tip-to-ring delta resistance in ohms for a copper loop test (CLT) module dc-delta resistance test.

**Usage** Read-only numeric field with a range of 0 to 4294967295. The value 99999999 indicates that the measurement is over range.

**Example** `dc-delta-resistance-t-r = 1200`

**Location** `CLT-RESULT`

**dc-delta-resistance-t-s**

**Description** Read-only. Indicates the tip-to-shield delta resistance in ohms for a copper loop test (CLT) module dc-delta resistance test.

**Usage** Read-only numeric field with a range of 0 to 4294967295. The value 99999999 indicates that the measurement is over range.

**Example** `dc-delta-resistance-t-s = 1200`

**Location** CLT-RESULT

**dc-delta-voltage-r-s**

**Description** Read-only. Indicates the ring-to-shield voltage in millivolts for a copper loop test (CLT) module dc-delta voltage test.

**Usage** Read-only numeric field with a range of 0 to 4294967295.

**Example** `dc-delta-voltage-r-s = 200`

**Location** CLT-RESULT

**dc-delta-voltage-t-s**

**Description** Read-only. Indicates the tip-to-shield voltage in millivolts for a copper loop test (CLT) module dc-delta voltage test.

**Usage** Read-only numeric field with a range of 0 to 4294967295.

**Example** `dc-delta-voltage-t-s = 200`

**Location** CLT-RESULT

**dcen392-val**

**Description** Specifies the total number of errors that must occur during data circuit-terminating equipment (DCE)-N392-monitored events to cause the network side to declare the user side's procedures inactive.

**Usage** Specify a value from 1 to 10. The value you specify must be less than the `dcen393-val` value. The default is 3.

**Example** `set dcen392-val = 7`

**Dependencies** If `link-type` is set to `dte`, `dcen392-val` does not apply.

**Location** FRAME-RELAY

## dcen393-val

**Description** Specifies the data circuit-terminating equipment (DCE)-monitored event count.

**Usage** Specify a value from 1 to 10. The value you specify must be greater than the value of dcen392-val. The default is 4.

**Example** `set dcen393-val = 8`

**Dependencies** If link-type is set to dte, dcen393-val does not apply.

**Location** FRAME-RELAY

## d-channel-enabled

**Description** Read-only. Indicates whether the unit enables D-channel (ISDN) signaling.

**Usage** The d-channel-enabled setting is read-only. Valid values are as follows:

- `yes`—Indicates that the unit supports D-channel signaling.
- `no`—Indicates that the unit does not support D-channel signaling.

**Example** `d-channel-enabled = yes`

**Location** BASE

## dead-interval

**Description** Specifies the number of seconds the Open Shortest Path First (OSPF) router waits for Hello packets before determining that its neighbor is unavailable.

**Usage** Specify a number from 0 through 65535. The default is 40 for a connected route, and 120 for a WAN connection.

**Example** `set dead-interval = 40`

**See Also** CONNECTION:ip-options:ospf-options  
IP-INTERFACE:ospf  
OSPF-VIRTUAL-LINK

## decrement-channel-count

**Description** Specifies the number of channels the Stinger unit removes as a bundle when bandwidth changes, either manually or automatically, during a call.



**Note** You cannot clear a call by decrementing channels.

**Usage** Specify an integer from 1 to 32. The default is 1.

**Example** `set decrement-channel-count = 2`

**Location** ANSWER-DEFAULTS:mpp-answer  
CONNECTION:mpp-options

## default-filter-cache-time

**Description** Specifies the number of minutes to cache RADIUS filter profiles that do not include a value for *Ascend-Cache-Time* (57).

Once the cache timer expires, cached profiles are deleted from system memory. The next time a remote filter is needed, the system retrieves the profile from RADIUS and stores it in cache again. Keeping a profile in cache increases performance when establishing sessions that use the filter, at the cost of some system memory.

**Usage** Specify a number of minutes. The default is 1440 (24 hours). If this parameter is set to 0 (zero), the default timer is disabled so that only RADIUS profiles specifying a cache time are cached.

**Example** `set default-filter-cache-time = 600`

**Dependencies** The system uses this setting only if no cache time is specified in the RADIUS filter profile.

**Location** IP-GLOBAL

## default-prt-cache-time

**Description** Specifies the number of minutes to cache RADIUS private-route profiles that do not include a value for *Ascend-Cache-Time* (57).

Keeping a profile in cache increases the performance of route lookups, at the cost of some system memory. Once the cache timer expires, cached profiles are deleted from system memory. The next time a private route is needed, the system retrieves the profile from RADIUS and stores it in cache again.

**Usage** Specify a number of minutes. The default is 1440 (24 hours). If this parameter is set to 0 (zero), the default timer is disabled so that only RADIUS profiles specifying a cache time are cached.

**Example** `set default-prt-cache-time = 600`

**Dependencies** The system uses this setting only if no cache time is specified in the RADIUS private-route profile.

**Location** IP-GLOBAL

## default-status

**Description** Specifies whether the Stinger unit displays the status screen by default when the user logs in.

**Usage** Valid values are as follows:

- **yes**—Specifies that the Stinger unit displays the status screen when it authenticates the profile.
- **no**—Specifies that the Stinger unit does not display the status screen when it authenticates the profile. This is the default.

**Example** `set default-status = yes`

**Dependencies** The default-status setting applies to Telnet and console logins. It does not apply to use of the auth command.

**Location** USER

## defect-ratio

**Description** *Not used.* Specifies the ratio of “no-defect-to-defect” time on a link. This parameter determines the relationship between the following:

- The amount of time the Stinger system waits to declare *no defect*
- The amount of time it waits before declaring a defect

The higher the value, the greater the integration time needed before the link can be used after it is out of alarms.

**Usage** Enter a number between 0 (zero) and 2147483647. The default is 10.

**Example** The following example specifies that five times as much time must elapse before the unit declares *no defect* and can use the link again.

```
set defect-ratio = 5
```

**Location** DS1-ATM:line-config:ima-option-config:rxlink-config

## delay

**Description** *Not used.*

## delay-callback

**Description** *Not supported.* Specifies a delay (in seconds) before the system initiates callback.

**Location** CONNECTION:telco-options

## delta-cell-delin-value

**Description** Specifies the number of consecutive cells with a correct header error count (HEC) required for the Stinger unit to move from the PRESYNC state to the SYNC state.

**Usage** Specify a number between 1 (one) and 16. The default is 6.

**Example**

```
set delta-cell-delin-value = 16
```

**Location** IMAHW-CONFIG

## desired-state

**Description** Specifies the desired administrative state of a device.

The actual state of the device can differ from the desired state, as when a device is starting (powering up), or if you change the desired state on a running slot. Changing the desired state does not force a device to the new state. It directs the Stinger unit to change the device state in a graceful manner.

**Usage** Valid values are as follows:

- `admin-state-down`—Specifies that the addressed device should terminate all operations and enter the DOWN state.
- `admin-state-up` (the default)—Specifies that the addressed device should come up in normal operations mode.

**Dependencies** You can change the administrative state of a device by using the SNMP Set commands or the Stinger `slot-d` and `slot-u` commands.

**Example** `set desired-state = admin-state-down`

**Location** ADMIN-STATE-PERM-IF  
ADMIN-STATE-PHYS-IF

## desired-trap-state

**Description** Read-only. Indicates whether `linkUp` and `linkDown` notifications (traps) have been enabled.

**Usage** The `desired-trap-state` setting is read-only. Valid values are as follows:

- `trap-state-enabled`—Indicates that `linkUp` and `linkDown` traps are generated for the interface.
- `trap-state-disabled`—Indicates that `linkUp` and `linkDown` traps are not generated for the interface.
- `system-defined` (the default)—Indicates that whether `linkUp` and `linkDown` traps are generated is determined in the system profile.

**Example** `desired-trap-state = trap-state-enabled`

**Location** ADMIN-STATE-PERM-IF  
ADMIN-STATE-PHYS-IF

## dest-address

**Description** Specifies a destination IP address in the following profiles:

- In an `ip-route` profile or the route description in a `private-route-table` profile, the default null address (0.0.0.0) represents the default route. The system forwards packets whose destinations do not match an entry in the routing table to the default route.
- In a filter profile, the combined value of `dest-address` and `dest-address-mask` represents a destination address to be filtered. The default null address (0.0.0.0) matches all packets.



**Usage** Specify an IP address in dotted decimal notation.

**Example** `set dest-address = 1.1.1.1`

**Dependencies** In a filter profile, this setting applies only if `type` is set to `ip-filter` or `tos-filter`.

**Location** `FILTER:input-filters[n]:ip-filter`  
`FILTER:output-filters[n]:ip-filter`  
`FILTER:input-filters[n]:tos-filter`  
`FILTER:output-filters[n]:tos-filter`  
`IP-ROUTE`  
`PRIVATE-ROUTE-TABLE`

## dest-address-mask

**Description** Specifies a mask that the system applies to the `dest-address` value before comparing that value to the destination address of a packet.

You can use this value to hide the host portion of an address, or its host and subnet portion. After translating the mask and address into binary format, the system applies the mask to the address by performing a logical AND operation. The mask hides the portion of the address that appears behind each binary 0 (zero) in the mask.

**Usage** Specify a mask in decimal notation. The default is 0.0.0.0, which masks all bits. A mask of all ones (255.255.255.255) masks no bits, so the system compares the full destination address of a single host.

**Example** `set dest-address-mask = 255.255.255.255`

**Dependencies** This setting applies only if the `type` parameter in the `input-filter` or `output-filter` subprofile is set to `ip-filter` or `tos-filter`.

**Location** `FILTER:input-filters[n]:ip-filter`  
`FILTER:output-filters[n]:ip-filter`  
`FILTER:input-filters[n]:tos-filter`  
`FILTER:output-filters[n]:tos-filter`

## destination-ip-address

**Description** Destination IP address.

**Usage** IP address. After applying the `destination-ip-netmask` to this value, a comparison is done. The default value is 0.0.0.0/0.

**Example** `set destination-ip-address = 192.168.0.3`

**Dependencies** If the destination address of the packet does not match the `destination-ip-netmask` of the rule, the comparison fails.

**Location** `PACKET-FLOWS/"":flow[n]:packet-classifier`

## destination-ip-netmask

**Description** Mask to be applied to the destination-ip-address value before a comparison is done.

**Usage** IP address. The default value is 0.0.0.0.

**Example** `set source-ip-netmask = 255.255.255.255`

**Dependencies** If the destination address of the packet does not match the destination-ip-address of the rule, the comparison fails.

**Location** `PACKET-FLOWS/"":flow[n]:packet-classifier`

## destination-mac-address

**Description** A destination MAC address.

**Usage** A six-byte hexadecimal number uniquely representing the destination host. The system will forward or discard packets addressed to this host, depending on how the filter is defined.

**Example** `set destination-mac-address = 12:34:56:78:9a:bc`

## destination-port

**Description** Number to be compared to the destination port of a packet when ip-protocol has been set to 17 (UDP) or 6 (TCP).

**Usage** If a nonzero destination-port is specified in a packet-flow profile, the ip-protocol value must be set to either 17 (UDP) or 6 (TCP). TCP and UDP port numbers are typically assigned to services. For a list of well-known port assignments, see RFC 1700, *Assigned Numbers*. The default value is 0.

**Example** `set destination-port = 6`

**Dependencies** If the destination address of the packet does not compare as specified to the destination-port of the rule, the comparison fails.

**Location** `PACKET-FLOWS/"":flow[n]:packet-classifier`

## destination-port-comparison

**Description** Operator to use in the destination-port comparison.

**Usage** The following operators can be used to compare destination port values:

- none (no comparison is made)
- equal (equal to)
- less (less than)
- greater (greater than)

The default value is none.

**Example** `set destination-port-comparison = less`

**Location** `PACKET-FLOWS/"" :flow[n] :packet-classifier`

## dest-port

**Description** Specifies the port number to be compared with the destination port of a packet. TCP and UDP port numbers are typically assigned to services.

For a list of assigned port numbers, see RFC 1700, *Assigned Numbers*, by Reynolds, J. and Postel, J., October 1994.

**Usage** Specify a number from 0 to 65535. The default is 0 (zero), which matches any port.

**Example** `set dest-port = 25`

**Dependencies** This setting applies only if type parameter in the input-filter or output-filter subprofile is set to ip-filter or tos-filter.

**Location** `FILTER:input-filters[n] :ip-filter`  
`FILTER:output-filters[n] :ip-filter`  
`FILTER:input-filters[n] :tos-filter`  
`FILTER:output-filters[n] :tos-filter`

## detect-end-of-packet

**Description** Enables or disables detection of the end of a packet.

**Usage** Valid values are as follows:

- `yes`—Specifies that end-of-packet detection is enabled.
- `no`—Specifies that end-of-packet detection is not enabled. This is the default.

**Example** `set detect-end-of-packet = yes`

**Location** `CONNECTION:tcp-clear-options`

## detection-interval

**Description** Specifies the detection interval in milliseconds for continuous detection. The system attempts to detect any abnormality at the defined milliseconds interval.

**Usage** The recommended value is 100ms (the default) for control modules. Valid values range from 0 (zero) to 65535.

**Example** `set detection-interval = 100`

**Location** `SYSTEM INTEGRITY:integrity-config`

## device-address

**Description** Specifies the three-part address of a module, in the format { shelf slot item }:

**Syntax element Description**

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| shelf | Specifies the shelf in which the item resides. For a Stinger unit, the shelf number is always 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| slot  | Specifies the number of the item's slot physical or virtual slot, as follows: <ul style="list-style-type: none"> <li>■ On a <i>Stinger FS</i> or <i>Stinger FS+</i>, line interface module (LIM) slots are numbered from 1 to 16 in the front of the unit, starting on the left. Slots 8 and 9 in the center are reserved for the control modules. Trunk modules reside in the center slots at the back of the unit, which have the virtual slot numbers 17 and 18.</li> <li>■ On a <i>Stinger LS</i> or <i>Stinger RT</i>, LIM slots are numbered from 1 to 5 (Model 1) or from 1 to 7 (Model 2), starting on the left. Slots 8 and 9 are reserved for the control modules, and slots numbered 17 and 18 at the far right are reserved for trunk modules. All physical slots are in the front of the unit.</li> <li>■ On a <i>Stinger MRT</i>, the built-in ADSL LIM resides in virtual slot 1, and the built-in control module is in virtual slot 8. The built-in STS-3 trunk interface resides in virtual slot 17, and the single trunk module is in a physical slot numbered slot 18.</li> </ul> |
| item  | Specifies the item on the module. Items are numbered starting with 1 for the topmost or leftmost item on the module. An item number of 0 (zero) denotes the entire slot. For example: <ul style="list-style-type: none"> <li>■ In a <i>Stinger FS</i>, <i>Stinger FS+</i>, <i>Stinger LS</i>, or <i>Stinger RT</i>, line 48 on a LIM in slot 2 has the following address: { 1 2 48 }.</li> <li>■ In a <i>Stinger MRT</i>, line 4 on a T1 trunk module has the following address: { 1 18 4 }</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Usage** In most cases, the device-address value is obtained from the system. However, you can clone a profile by reading an existing one and changing its device address. Valid values are as follows:

- For shelf—shelf-1 only
- For slot—a value from slot-1 through slot-18
- For item-number—an integer in the range 0 (indicating the entire slot) through the total number of interfaces on the module

**Example** The following example shows a listing of the device address for interface 37 on a LIM in slot 9 of a Stinger FS, and demonstrates how to change the slot number to 2:

```
admin> list device-address
[in ADMIN-STATE-PHYS-IF { shelf-1 slot-9 37 }]
shelf = shelf-1
slot = slot-9
item-number = 37
admin> set slot = slot-2
```

As an alternative, you can use only the set command. For example:

```
admin> set device-address slot = slot-2
```

**Location** ADMIN-STATE-PHYS-IF  
DEVICE-STATE  
TRUNK-DAUGHTER-DEV

## device-state

**Description** Read-only. Indicates the current operational state of a device.

**Usage** The device-state value is read-only. The following are valid values:

For the device-state profile:

- down-dev-state—Indicates that the device is in a nonoperational state.
- up-dev-state—Indicates that the device is in normal operations mode.
- none-dev-state—Indicates that the device does not currently exist.
- restart-dev-state—The addressed device is being restarted.

For the trunk-daughter-dev profile:

- trunk-daughter-oper-state-down—The device is down, a non-operational state.
- trunk-daughter-oper-state-up—The device is in a normal operations mode.
- trunk-daughter-oper-state-none—The device does not exist; the daughter card slot is empty.
- trunk\_daughter\_number-of-states

**Example** device-state = up-dev-state

**Location** DEVICE-STATE  
TRUNK-DAUGHTER-DEV

## device-type

**Description** Type of device advertised in Integrated Local Management Interface (ILMI). *ILMI is not supported with the current software version.*

**Usage** Valid values are as follows:

- private (default)
- public

**Example** set device-type = public

**Location** ATM-IF-CONFIG:extension-config

## dev-line-state

**Description** Read-only. Indicates the status of the ADSL, HDSL2, SDSL, or SHDSL interface.

**Usage** The dev-line-state value is read-only. Valid values depend on the profile.

- ADSL values:
  - down—There is no connection, or the interface is disabled.
  - activation—The interface is attempting to train but is not yet detecting a modem at the other end.
  - training—The interface is training with a modem on the other end.
  - port-up—The interface successfully trained up.
  - failed—The interface failed training. (A log message specifies the reason.)
  - loopback—The interface is in loopback test mode.
- SDSL values:
  - config—The interface is being configured.
  - deactivate—The interface is transitioning to the DOWN state.
  - inactive—The interface is starting up.
  - activating—The interface is waiting for customer premises equipment (CPE) to start up.
  - active-rx—The interface is waiting for four-level transmission from CPE.
  - port-up—The interface is connected to CPE, and data can be transferred.
  - portup-pending-deactive—The interface has a loss-of-signal or noise-margin error (noise greater than -5dB).
  - deactivate-lost—The interface is waiting for loss-of-signal timer to expire.
  - hardware-test—A hardware self-test is in progress.
  - out-of-service—The interface is out of service.
  - tip-ring-detect—The interface is running a simple internal bit-error rate test (BERT) to detect correct tip-ring orientation.
  - forever-bert—The interface is running an internal BERT to detect correct tip-ring orientation.
  - tip-wait1—The interface is running an internal BERT to detect correct tip-ring orientation.
  - tip-hunt—The interface is running an internal BERT to detect correct tip-ring orientation.
  - tip-wait2—The interface is running an internal BERT to detect correct tip-ring orientation.
  - cell-delineation—The interface is attempting to recover ATM cells (idle cells as well as data cells) from the receiving octets. If recovery is successful, the interface transitions to the UP state.

- deactivate-wait—The interface is waiting to transition to the DOWN state.
- SHDSL and HDSL2 values:
  - port-up—Connected to CPE and data can be transferred.
  - test—Line is in test mode.
  - start-up-handshake—Startup handshake is occurring.
  - start-up-training—Startup training is occurring.
  - start-up-download—Startup download is occurring.
  - idle—Line is idle.
  - down—Line is not currently operational.
  - out-of-service—Line is out of service.
  - unknown—Line status is unknown.
  - analog-loopback—Line is in analog loopback mode.
  - digital-loopback—Line is in digital loopback mode.

**Example** dev-line-state = port-up

**Location** AL-DMT-STAT:physical-status  
HDSL2-STAT:physical-status  
SHDSL-STAT:physical-status  
SDSL-STAT:physical-status

## dhcp-allow-any-src-port

**Description** Process and allow DHCP requests from a nonstandard source port, and add option 82 to such requests.

**Usage** Valid values are as follows:

- yes—Enable this feature.
- no—Disable this feature. This is the default.

**Example** set dhcp-allow-any-src-port = yes

**Location** IP-GLOBAL:bootp-relay:relay-agent-information:circuit-id  
IP-GLOBAL:bootp-relay:relay-agent-information:remote-id  
BRIDGE-GROUP:dhcp-snooping:circuit-id  
BRIDGE-GROUP:dhcp-snooping:remote-id  
BRIDGE-GROUP:pppoe-snooping:circuit-id  
BRIDGE-GROUP:pppoe-snooping:remote-id

## dial-number

**Description** *Not supported.* Specifies the type of telephone number used to dial out a call.

**Location** CONNECTION

## dial-on-broadcast

**Description** *Not supported.* Specifies whether the system attempts to establish a bridged connection on the interface when it receives a frame whose media access control (MAC) address is set to broadcast.

**Location** CONNECTION:bridging-options  
ETHERNET:bridging-options

## dialout

**Description** Specifies the password for a dial-out pseudo-user.

**Usage** Enter a password of up to 21 characters.

**Example** set dialout = mypass

**Location** EXTERNAL-AUTH:password-profile

## dialout-auth-lns

**Description** *Not supported.* Specifies the ability of the Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) to accept dial-out requests only from the L2TP network server (LNS) that was authenticated during the tunnel setup.

**Usage** Valid values are as follows:

- yes—Restricts the LAC to accept dial-out requests from only the LNS that was authenticated during tunnel setup.
- no—Allows the LAC to accept dial-out requests from an LNS other than the one that was authenticated during tunnel setup.

**Location** L2-TUNNEL-GLOBAL:l2tp-config

## dialout-number-auth

**Description** Enables or disables calling line ID (CLID) authorization for the dial-out number passed by the Layer 2 Tunneling Protocol (L2TP) network server (LNS).

**Usage** Valid values are as follows:

- no—Disables CLID authorization. This is the default.
- yes—Enables CLID authorization.

**Example** set dialout-number-auth = yes

**Location** TUNNEL-SERVER:dialout-options



## dialout-poison

**Description** Enables or disables advertisement of dial-out routes when no trunks are available. Disabling advertisement (the `yes` setting) allows a redundant unit to take over.

**Usage** Specify `yes` or `no`. The default is `no`.

- `yes`—Stop advertising the system's IP dial-out routes if no trunks are available.
- `no`—Continue to advertise the unit's dial-out routes, even if no trunks are currently available. This is the appropriate setting for Stinger units, which do not use dial-out routes.

**Example** `set dialout-poison = no`

**Location** `IP-GLOBAL`

## dialout-routes

**Description** Specifies the password for the dial-out route's pseudo-user.

**Usage** Enter a password of up to 21 characters.

**Example** `set dialout-routes = mypass`

**Location** `EXTERNAL-AUTH:password-profile`

## dialout-send-profile-name

**Description** *Not supported.* Specifies whether the Layer 2 Tunneling Protocol (L2TP) network server (LNS) can send the connection profile name vendor-specific attribute along with the dial-out request.

**Location** `L2-TUNNEL-GLOBAL:l2tp-config`

## diff-delay-max

**Description** Specifies the permissible range of differential delay for inverse multiplexing over ATM (IMA) groups, expressed in milliseconds (msecs).

**Usage** The default is 25. To determine the maximum differential delay among the lines in a group, subtract the smallest delay from the largest.

- For a T1 module, the range is from 0 (zero) to 281 msecs.
- For an E1 module, the range is from 0 to 225 msecs. If a value greater than 225 is specified for an E1 module, the system allows you to write the profile, but when the IMA group negotiation begins on the module, the differential delay is limited to the maximum permitted value (225 msecs) and the system logs the following message:

`IMAGROUP <groupName> has invalid differential delay(%d)-using 225 msecs`

**Example** The following command sets the maximum differential delay for an IMA group in which line 1 has a delay of 10ms, line 2 has a delay of 25ms and line 3 has a delay of 5ms. The maximum differential delay among the three lines is 25 minus 5, or 20ms.

```
set diff-delay-max = 20
```

**Location** IMAGROUP

## diff-delay-max-obs

**Description** Read-only, Indicates the latest maximum differential delay observed (in milliseconds) between the links having the least and most link propagation delay, among the receive links that are currently configured in the inverse multiplexing over ATM (IMA) group.

**Usage** The diff-delay-max-obs value is read-only. Valid values range from 0 (zero) to 2147483647.

**Example** diff-delay-max-obs = 0

**Location** IMA-GROUP-STAT

## direct

**Description** *Not used.*

## direct-access

**Description** *Not used.*

## directed-broadcast-allowed

**Description** Enables or disables forwarding of directed broadcast traffic onto the interface and its network.

Denial-of-service attacks known as “smurf” attacks typically use Internet Control Message Protocol (ICMP) Echo Request packets with a spoofed source address and packets directed to IP broadcast addresses. These attacks are intended to degrade network performance, possibly to the point that the network becomes unusable. This setting can prevent the IP router from being used as an intermediary in this type of denial-of-service attack launched from another network

**Usage** Valid values are as follows:

- yes (the default)—Allows the system to forward directed broadcasts received from another network.
- no—Prevents the router from forwarding directed broadcasts it receives from another network.



**Note** To protect against the router being used in a denial-of-service attack, you must prevent the router from forwarding directed broadcasts it receives from another network on *all* IP interfaces in the system. For example, you must disable directed broadcasts on both control-module interfaces (so the broadcasts are still disabled if controller switchover occurs), as well as the IP interfaces of a router module.

**Example** `set directed-broadcast-allowed = no`

**Location** IP-INTERFACE

## direction-mode

**Description** Specifies (in the `aps-config` profile) and indicates (in the `aps-stat` profile) whether the protection group's mode of direction is unidirectional or bidirectional in automatic protection switching (APS).

**Usage** Valid values are as follows:

- `unidirectional`—The end having the failure switches to the protection channel without communicating to the other end first. The decision to switch is unilateral. This is the default and is recommended for APS 1+1.
- `bidirectional`—When a failure occurs, it is communicated to the opposite end and both ends determine whether to switch to the protection channel.

**Example** `set direction-mode = unidirectional`

**Location** APS-CONFIG  
APS-STAT

## disabled-count

**Description** *Not used.*

## disconnect-on-auth-timeout

**Description** Specifies how the Stinger unit disconnects a PPP connection if it times out while waiting for RADIUS authentication.

**Usage** Valid values are as follows:

- `yes` (the default)—Instructs the unit to hang up a PPP connection if RADIUS authentication times out.
- `no`—Instructs the unit to disconnect cleanly after a RADIUS time-out.

**Example** `set disconnect-on-auth-timeout = yes`

**Location** ANSWER-DEFAULTS:ppp-answer  
CONNECTION:ppp-options

## dlci

**Description** Specifies or indicates, according to the profile, a data link connection identifier (DLCI) number for a frame relay connection.

A DLCI is not an address, but a local label that identifies a logical link between a device and the frame relay switch. The switch uses the DLCI to route frames through the network, and the DLCI can change as frames are passed through multiple switches.

**Usage** Valid values are as follows:

- For a fr-options subprofile, specify an integer from 16 through 991. The default is 16. Ask your frame relay network administrator for the value you must enter.
- For a dlci-ident or dlci-member[n] subprofile, this setting is a read-only value up to 15 characters long.

**Example** set dlci = 17

**Dependencies** Consider the following:

- For dlci to apply, fr-direct-enabled must be set to no.
- The dlci setting is ignored for a connection profile that has circuit-type set to svc. For a switched virtual circuit (SVC), the DLCI value is assigned to the circuit by the network. The range of DLCI values for circuits is shared between permanent virtual circuits (PVCs) and SVCs, and is managed between the network and user entities.

**Location** CONNECTION:fr-options

FRDLCI-STAT:dlci-ident

FRPVC-STAT:dlci-members:dlci-member:[n]

## dlci-route-id

**Description** Read-only. Indicates the system route ID value associated with a DLCI.

**Usage** Read-only numeric value with a range of 0 to 65535.

**Example** dlci-route-id = 1818

**Location** FRDLCI-STAT:dlci-ident

FRPVC-STAT:dlci-members[n]

## dmmall-input-imp

**Description** Specifies the input impedance, in kilohms, for a digital multimeter (DMM) copper loop test (CLT).

**Usage** Specify either 100 or 1000kohms.

**Example** set dmmall-input-imp = 100

**Location** CLT-COMMAND

## `dmmall-period`

**Description** Specifies the amount of time, in tenths of a second, during which measurement is made in a digital multimeter (DMM) copper loop test (CLT).

**Usage** Specify a number between 0 (zero) and 5. The default value, 0, sets the maximum time period. Values between 1 and 5 set times between 100ms and 500ms.

**Example** `set dmmall-period = 1`

**Location** CLT-COMMAND

## `dmm-all-r-s`

**Description** Read-only. Indicates the ring-to-shield measurement data for a copper loop test (CLT) module digital multimeter test.

**Usage** Read-only numeric value with a range of 0 to 4294967295. Volts dc and volts ac are in millivolts. Resistance is in ohms. Capacitance is in picofarads.

**Example** `dmm-all-r-s = 1220`

**Location** CLT-RESULTS

## `dmm-all-t-r`

**Description** Read-only. Indicates the tip-to-ring measurement data for a copper loop test (CLT) module digital multimeter test.

**Usage** Read-only numeric value with a range of 0 to 4294967295. Volts dc and volts ac are in millivolts. Resistance is in ohms. Capacitance is in picofarads.

**Example** `dmm-all-t-r = 1220`

**Location** CLT-RESULTS

## `dmm-all-t-s`

**Description** Read-only. Indicates the tip-to-shield measurement data for a copper loop test (CLT) module digital multimeter test.

**Usage** Read-only numeric value with a range of 0 to 4294967295. Volts dc and volts ac are in millivolts. Resistance is in ohms. Capacitance is in picofarads.

**Example** `dmm-all-t-s = 1220`

**Location** CLT-RESULTS

## *dmmall-type*

**Description** Specifies the type of digital multimeter (DMM) cooper loop test (CLT) to run for all measurements: tip to ring, tip to ground, and ring to ground.

**Usage** Valid values are as follows:

- *resistance*—Measures dc resistance to detect shorts and leakage between tip and ring, tip and ground, and ring and ground.
- *dc-voltage*—Measures dc voltage to detect unwanted foreign voltage.
- *ac-voltage*—Measures ac voltage to detect unwanted foreign voltage.
- *capacitance*—Measures actual capacitance and estimated length for loop-length estimation.

**Example** `set dmmall-type = resistance`

**Location** CLT-COMMAND

## *dmmcap-period*

**Description** Specifies the amount of time, in tenths of a second, during which measurement is made in a digital multimeter (DMM) copper loop test (CLT) that measures capacitance.

**Usage** Specify a number between 0 (zero) and 5. The default value, 0, sets the maximum time period. Values between 1 and 5 set times between 100ms and 500ms.

**Example** `set dmmcap-period = 2`

**Location** CLT-COMMAND

## *dmdcd-impedance*

**Description** Specifies the output impedance, in kilohms, to be used in a digital multimeter (DMM) copper loop test (CLT) that measures loop resistance based on a dc Thevenin circuit.

**Usage** Specify a number between 10 and 1000. The default is 10.

**Example** `set dmdcd-impedance = 1000`

**Location** CLT-COMMAND

## `dmmdcd-period`

**Description** Specifies the amount of time, in tenths of a second, during which measurement is made in a digital multimeter (DMM) copper loop test (CLT) that measures loop resistance based on a dc Thevenin circuit.

**Usage** Specify a number between 1 (one) and 5. Each unit represents 100 milliseconds. Enter the default 0 (zero) value for the maximum time.

**Example** `set dmmdcd-period = 1`

**Location** CLT-COMMAND

## `dmmdcd-voltage`

**Description** Specifies the test voltage to be used in a digital multimeter (DMM) copper loop test (CLT) that measures loop resistance based on a dc Thevenin circuit.

**Usage** Specify a number between -230 and 230. The default is 0 (zero).

**Example** `set dmmdcd-voltage = 230`

**Location** CLT-COMMAND

## `dmm-lead`

**Description** Specifies the digital multimeter (DMM) measurement leads to be used in a copper loop test (CLT).

**Usage** Valid values are as follows:

- `tip-ring`—Measures between tip and ring (lead T-R.) This is the default.
- `tip-sleeve`—Measures between tip and ground (lead T-S).
- `ring-sleeve`—Measures between ring ground (lead R-S).

**Example** `set dmm-lead = tip-sleeve`

**Location** CLT-COMMAND

## `dmm-result`

**Description** Read-only. Indicates the results of a digital multimeter (DMM) copper loop test (CLT).

**Usage** The `dmm-result` value is read-only. V

- Voltage ac and dc are reported in millivolts.
- Resistance is reported in ohms.
- Capacitance is reported in nanofarads.

**Example** `dmm-result = 0`

**Location** CLT-RESULT

*dmm-type*

**Description** Specifies the type of digital multimeter (DMM) copper loop test (CLT) to run.

**Usage** Valid values are as follows:

- *resistance* (the default)—Measures dc resistance to detect shorts and leakage between tip and ring, tip and ground, and ring and ground.
- *dc-voltage*—Measures dc voltage to detect unwanted foreign voltage.
- *ac-voltage*—Measures ac voltage to detect unwanted foreign voltage.
- *capacitance*—Measures actual capacitance and estimated length for loop-length estimation.

**Example** `set dmm-type = capacitance`

**Location** CLT-COMMAND

*dns-list-attempt*

**Description** Enables or disables the Domain Name System (DNS) list feature.

DNS lists allow the system to return multiple IP addresses to Telnet clients at sites where DNS responds with more than one address. The system stores the hostname/address associations in the local DNS table in RAM, overwriting configured addresses in that table or addresses received from earlier DNS queries. To prevent stale entries in the table in RAM, the system clears the number of addresses exceeding the amount specified by *dns-list-size*.

If the DNS list feature is disabled, the system stores a single returned address in the local DNS table in RAM, clearing the remaining 34 hostname/address fields.

**Usage** Valid values are as follows:

- *yes*—Returns multiple addresses if available, up to the limit specified by *dns-list-size*.
- *no*—Returns only one address from any successful DNS query. This is the default.

**Example** `set dns-list-attempt = yes`

**Location** IP-GLOBAL



## dns-list-size

**Description** Specifies the maximum number of hosts in a Domain Name System (DNS) list, up to 35.

If the DNS list feature is enabled and DNS returns multiple addresses, this setting determines the number of addresses displayed for a Telnet client.

**Usage** Enter a number from 0 to 35. The default is 6.

**Example** `set dns-list-size = 10`

**Dependencies** If `dns-list-attempt` is set to no, `dns-list-size` has no effect.

**Location** IP-GLOBAL

## dns-primary-server

**Description** Specifies the IP address of the primary local Domain Name System (DNS) server to use for lookups.

**Usage** Specify an IP address in dotted decimal notation.

**Example** `set dns-primary-server = 2.2.2.2/28`

**Dependencies** When specified in a `vrouter` profile, this DNS setting is exclusive to the virtual router. If DNS settings are not specified in a `vrouter` profile, the virtual router uses the DNS settings defined in the `ip-global` profile.

**Location** IP-GLOBAL  
VROUTER

## dns-secondary-server

**Description** Specifies the IP address of the secondary local Domain Name System (DNS) server to use for lookups. This DNS setting is used only if the primary server is not found.

**Usage** Specify an IP address in dotted decimal notation.

**Example** `set dns-secondary-server = 2.2.2.4/28`

**Dependencies** When specified in a `vrouter` profile, this DNS setting is exclusive to the virtual router. If DNS settings are not specified in a `vrouter` profile, the virtual router use the DNS settings defined in the `ip-global` profile.

**Location** IP-GLOBAL  
VROUTER

## dns-server-query-type

**Description** Specifies how to query a Domain Name System (DNS) server.

**Usage** Valid values are as follows:

- `udp`—Queries the DNS server first by means of UDP, and then, if the TC-bit is set and a retry is necessary, by means of TCP. This is the default.
- `udp-ignore-tc-bit`—Queries the DNS server only by means of UDP.
- `tcp`—Queries the DNS server only by means of TCP.
- `tcp-keep-open`—Queries the DNS server by means of TCP only and then attempts to keep the TCP session established, rather than opening a new TCP session for each additional query.

**Example** `set dns-server-query-type = tcp`

**Location** IP-GLOBAL

## domain-name

**Description** Specifies the primary domain name to use for Domain Name System (DNS) lookups. The system appends this domain name to hostnames when performing lookups.

**Usage** Specify a domain name.

**Example** `set domain-name = abc.com`

**Dependencies** When specified in a `vrouter` profile, this DNS setting is exclusive to the virtual router. If DNS settings are not specified in a `vrouter` profile, the virtual router use the DNS settings defined in the `ip-global` profile.

**Location** IP-GLOBAL  
VROUTER

## domestic-enabled

**Description** Read-only. Indicates whether a Stinger unit can operate domestically.

**Usage** Read-only parameter with the following possible values:

- `no`—Unit cannot operate domestically.
- `yes`—Unit can operate domestically.

**Example** `domestic-enabled = no`

**Location** BASE

## door-open

**Description** An alarm was received from the remote shelf fan to indicate that the door is open.

**Usage** This parameter is read-only. Valid values are as follows:

- yes—An alarm was received.
- no (the default)—No alarms were received.

**Location** REMOTE-SHELF-STAT

## do-version-fallback

**Description** Specifies whether the Stinger unit automatically falls back to the earlier version of inverse multiplexing ATM (IMA) if the far-end Stinger unit is detected to be running the earlier version.

**Usage** Valid values are as follows:

- yes—Specifies that the unit falls back from version 1.1 to version 1.0.
- no—Specifies that the unit does not fall back, but moves to the configAborted state. This is the default.

**Example** set do-version-fallback = yes

**Location** IMAGROUP

## down-cost

**Description** Specifies the Open Shortest Path First (OSPF) output cost when the link is physically down but virtually up.

**Usage** Specify a value from 1 through 16777215 (the default).

**Example** set down-cost = 1000

**Location** IP-INTERFACE:ospf  
CONNECTION:ip-options:ospf-options

## down-metric

**Description** Specifies the routing metric, typically measured in number of hops, to be used in the routing table entry created for this connection when the connection is inactive.

**Usage** Numeric parameter with a range of 1 to 15 hops. Default value is 7.

**Example** set down-metric = 12

**Location** CONNECTION:ip-options

## down-preference

**Description** Specifies a preference value for a route when the interface is unavailable. The system uses this value to determine when to bring a route online.

**Usage** Specify a number from 0 to 214748364. The lower the preference, the more likely the system is to bring the route online when interface is unavailable. The default is 120.

**Example** `set down-preference = 255`

**Location** `CONNECTION:ip-options`

## downstream-end-bin

**Description** Specifies the ending frequency bin (interval) for downstream transmission.

The upstream and downstream start and end bins define the frequency ranges for upstream and downstream data. The frequency for a particular bin is defined as follows:

$$\text{frequency} = \text{bin number} \times 4.3125\text{kHz}$$

You can use these parameters to adjust the frequency content of the ADSL signals. For example, splitterless ANSI discrete multitone (DMT) can be supported by appropriate adjustment of the frequency range.

**Usage** Valid values are as follows:

- For 12-port, 24-port, and 48-port Annex A line interface modules (LIMs), specify a number from 32 to 255. The default is 255.
- For 48-port G.lite LIMs, specify a number from 37 to 127. The default is 127.

**Example** `set downstream-end-bin = 50`

**Dependencies** You must adjust the maximum and minimum bit rate parameters to match the frequency range defined by the start and end bin numbers.

**Location** `AL-DMT:line-config`

## down-stream-latency

**Description** Read-only. Indicates the operational downstream latency setting.

**Usage** The `down-stream-latency` value is read-only. Valid values are as follows:

- `none`—Indicates that the line is not operational.
- `fast`—Indicates that the setting for least downstream delay is in effect.
- `interleave`—Indicates that interleave latency (greater than `fast`) is in effect

**Example** `down-stream-latency = interleave`

**Location** `AL-DMT-STAT:physical-status`

## down-stream-rate

**Description** Read-only. Indicates the downstream rate, in bits per second, for an SDSL line interface module (LIM) and port reported on.

**Usage** Read-only parameter with a numeric value of 0 to 4294967295bps.

**Example** down-stream-rate = 18282

**Location** SDSL-STAT:physical-status

## down-stream-rate-fast

**Description** Read-only. Indicates the downstream data rate in bits per second when latency is fast.

**Usage** The down-stream-rate-fast value is read-only. Zero (0) means that latency is set to interleave or that the data rate is unknown.

**Example** down-stream-rate-fast = 0

**Location** AL-DMT-STAT:physical-status

## down-stream-rate-interleaved

**Description** Read-only. Indicates the downstream data rate in bits per second when latency is interleave.

**Usage** The down-stream-rate-interleaved value is read-only. Zero (0) means that latency is set to fast or the data rate is unknown.

**Example** down-stream-rate-interleaved = 2944000

**Location** AL-DMT-STAT:physical-status

## downstream-start-bin

**Description** Specifies the starting downstream frequency bin (interval).

**Usage** Specify a number from 6 to 511 for ADSL2+ capable line interface modules(LIMs), for all other LIMs specify a number from 32 to 255. The default is 32.

**Example** set downstream-start-bin = 35

**Location** AL-DMT:line-config

## dr-capable

**Description** Enables/disables the neighboring router from being the designated router (yes or no).

**Usage** Valid values are as follows:

- yes—Enable.
- no (the default)—Disable.

**Example** `set dr-capable = yes`

**Location** OSPF-NEBA-NEIGHBOR

## drop-source-routed-ip-packets

**Description** Enables or disables forwarding of IP packets that have the source route option set.

**Usage** Valid values are the following.

- yes—Drop all packets that have a Loose or a Strict source route among their IP options.
- no (the default)—Forward all source-routed packets, as described in RFC 1812.

**Example** `set drop-source-routed-ip-packets = no`

**Location** IP-GLOBAL

## dscp

**Description** Specifies the differentiated services code point (DSCP) value.

**Usage** Specify a value from 00 (the default) to 3F (hexadecimal). DSCP marking, as defined in RFC 2474, uses the first 6 bits in the second octet in the IP datagram to create values (from 00 through 3F) specifying different classes of service:

| Bit positions | TOS-precedence (RFC 791)              | DSCP (RFC 2474)        |
|---------------|---------------------------------------|------------------------|
| 0 to 2        | Precedence (eight levels of priority) | DSCP value             |
| 3             | Delay (normal or low)                 | DSCP value (continued) |
| 4             | Throughput (normal or high)           | DSCP value (continued) |
| 5             | Reliability (normal or high)          | DSCP value (continued) |
| 6 to 7        | Reserved                              | Reserved               |

**Example** `set dscp = 3f`

**Dependencies** For this setting to apply, you must set the `marking-type` parameter to `dscp`. In addition, type-of-service (TOS) and IP routing must be enabled in the connection profile, or TOS must be specified as the filter type in the filter profile.

**Location** CONNECTION:ip-options:tos-options  
FILTER:input-filters:tos-filter  
FILTER:output-filters:tos-filter

## dsl-thresh-trap-enabled

**Description** Enables or disables sending of DSL traps (notifications) to the identified host.

**Usage** Specify one of the following values:

- `yes`—The system sends DSL traps to the identified host.
- `no`—The system does not send DSL traps to the identified host.

**Example** `set dsl-thresh-trap-enabled = yes`

**Location** TRAP

## dst-port-cmp

**Description** Specifies whether a filter tests for destination port numbers that are equal to a specified `dest-port` value, or port numbers that are less than, greater than, or not equal to the specified value.

**Usage** Valid values are as follows:

- `none` (the default)—Does not compare destination port numbers.
- `less`—Matches destination port numbers less than the `dest-port` value.
- `eq`—Matches destination port numbers equal to the `dest-port` value.
- `gtr`—Matches destination port numbers greater than the `dest-port` value.
- `neq`—Matches destination port numbers not equal to the `dest-port` value.

**Example** `set dst-port-cmp = eq`

**Dependencies** This setting applies only if the `type` parameter in the `input-filter` or `output-filter` subprofile is set to `ip-filter` or `tos-filter`.

**Location** FILTER:input-filters[n]:ip-filter  
FILTER:output-filters[n]:ip-filter  
FILTER:input-filters[n]:tos-filter  
FILTER:output-filters[n]:tos-filter

## dual-link

**Description** *Not currently used.*

**Location** IDSL:line-interface

## dual-slot-t1-enabled

**Description** Indicates whether all 8 T1 ports on the MRT trunk module are enabled.

**Usage** The following read only values are valid:

- `yes`—All T1 ports are enabled.
- `no`—All T1 ports are not enable.

**Dependencies** This parameter is only visible on a Stinger MRT.

**Location** `BASE`

## duplex-mode

**Description** Specifies the operating mode of the Stinger Ethernet LAN interface.

**Usage** Valid values are the following:

- `full-duplex` (the default)—Provides higher throughput.
- `half-duplex`—Enables the unit to operate with older equipment that does not support full duplex.

**Example** `set duplex-mode = half-duplex`

**Dependencies** The system can determine the proper setting for this parameter when `auto-negotiate` is set to `yes`.

**Location** `ETHERNET`

## dynamic-algorithm

**Description** Specifies the algorithm to use to calculate the average link utilization (ALU) over a specified number of seconds (`seconds-history`). After calculating the average, the Stinger unit compares it to the `target-utilization` value. If the average exceeds or falls below the target for a specified number of seconds, the unit adjusts the bandwidth of the connection.

**Usage** Valid values are as follows:

- `quadratic` (the default)—Specifies that more weight is given to recent samples of bandwidth usage than to older samples. The weighting grows at a quadratic rate.
- `linear`—Specifies that more weight is given to recent samples of bandwidth usage than to older samples. The weighting grows at a linear rate.
- `constant`—Specifies that equal weight is given to all samples.

**Example** `set dynamic-algorithm = linear`

**Location** `ANSWER-DEFAULTS:mpp-answer`  
`CONNECTION:mpp-options`



---

## E

### early-packet-discard

**Description** Specifies whether all cells in an asynchronous transfer mode (ATM) packet are discarded if the first cell cannot be queued.

**Usage** Valid values are as follows:

- **yes**—Specifies that the cell and all remaining cells are discarded. This is the default.
- **no**—Specifies that the cell and all remaining cells are not discarded. However, when the end of the current packet is detected, all the cells in the next packet are discarded. This is the default.

**Example** `set early packet-discard = no`

**Dependencies** If `encapsulation-protocol` is not set to `atm` or `atm-circuit`, the `early-packet-discard` setting does not apply.

**Location** `ATM-QOS`

### elapsed-seconds

**Description** Read-only. Indicates the number of seconds that have elapsed in the current measurement interval of 15 minutes.

**Usage** The `elapsed-seconds` value is read-only. Valid values range from 0 (zero) to 2147483647.

**Example** `elapsed-seconds = 0`

**Location** `DS1-ATM-STAT:ima-link-statistic`

### enable

**Description** Enables or disables a feature:

- In a `trunk-cac-config` subprofile, specifies whether connection admission control (CAC) is enabled on the port specified in `port-num` in this subprofile.
- In a `bir-options` subprofile, specifies whether bridged IP routing (BIR) is enabled on an interface.
- In a `ospf-global` profile, globally enables or disables Open Shortest Path First (OSPF) operation.
- In a `circuit-id` subprofile, enables or disables the circuit identifier suboption of DHCP option 82.
- In a `remote-id` subprofile, enables or disables the remote identifier suboption of DHCP option 82.
- In a `multiple-ip-address` subprofile enables or disables static configuration of multiple IP addresses for this BIR connection.

**Usage** Valid values are as follows:

- For the `trunk-cac-config` subprofile:
  - `yes`—Enables the feature. This is the default in `trunk-cac-config` subprofile.
  - `no`—Disables the feature.
- For the `bir-options` subprofile:
  - `yes`—Enables the feature.
  - `no`—Disables the feature. This is the default in a `bir-options` subprofile.
- For the `ospf-global` subprofile:
  - `yes`—Globally enables OSPF.
  - `no`—Globally disables OSPF. This is the default.
- For the `circuit-id` subprofile:
  - `yes`—Enables the circuit identifier suboption of DHCP option 82. The IP2000 encodes the `station` value (the hostname) of the `connection` or `RADIUS` profile that defines the PVC on which the DHCP client-to-server packet was received. This ensures that DHCP responses are sent back to the proper circuit.
  - `no` (the default)—Disables the circuit identifier suboption of DHCP option 82.
- For the `remote-id` subprofile:
  - `yes`—Enables the remote identifier suboption of DHCP option 82. The IP2000 encodes a globally unique identifier of the remote CPE from which it received a DHCP client-to-server packet, to ensure that DHCP responses are sent back to the proper remote client. The IP2000 can use this field in addition to or instead of the `circuit-id` field.
  - `no` (the default)—Disables the remote identifier suboption of DHCP option 82.
- For the `multiple-ip-address` subprofile:
  - `yes`—Activates all correctly configured WAN virtual interfaces configured in the `multiple-ip-address` subprofile. At least one `remote-address` field must be configured in the `multiple-ip-address` subprofile.
  - `no` (the default)—Deactivates all correctly configured WAN virtual interfaces configured in the `multiple-ip-address` subprofile.

**Example** `set enable = no`

**Dependencies** For the `trunk-cac-config` subprofile, when the OC3 interface is disabled, it transmits the OC3 Idle signal to the remote end.



**Note** The `trunk-cac-config:enabled` parameter was previously located in the `atm-config` profile. Its use in that location has been deprecated.

**Dependencies** For the `ospf-global` subprofile consider the following:

- After enabling OSPF routing, you must reset the system. The only time the system brings up OSPF routing on an interface is after a reset. As the system starts up with OSPF enabled on one or more interfaces, it begins to form adjacencies and build its routing table.
- If you are modifying many OSPF-related profiles, you can use the `enable` value to prevent OSPF from reinitializing several times. In this case, set `enable` to `no`, write the OSPF changes, and then set `enable` to `yes` again.

**Dependencies** In the multiple-ip-address subprofile this parameter cannot be set to yes if the bootp-relay-options enable setting is set to yes, and vice versa.

**Location** BRIDGE-GROUP

BRIDGE-GROUP:dhcp-snooping

BRIDGE-GROUP:dhcp-snooping:circuit-id

BRIDGE-GROUP:dhcp-snooping:remote-id

BRIDGE-GROUP:pppoe-snooping

BRIDGE-GROUP:pppoe-snooping:circuit-id

BRIDGE-GROUP:pppoe-snooping:remote-id

CONNECTION:bir-options

CONNECTION:bir-options:multiple-ip-address:ip-address-option[n]

HIGH-SPEED-SLOT-STATIC-CONFIG:trunk-cac-config

IP-GLOBAL:ospf-global

IP-GLOBAL:bootp-relay:relay-agent-information:circuit-id

IP-GLOBAL:bootp-relay:relay-agent-information:remote-id

## enable-centralized-detection

**Description** Specifies whether central integrity checking is enabled by the primary control module for the entire system.

**Usage** Valid values are as follows:

- yes—Enables central integrity checking.
- no (the default)—Disables central integrity checking. By default, line interface modules (LIMs) perform error correction, which is usually sufficient for most applications. .

**Example** set enable-centralized-detection = yes

**Location** SYSTEM-INTEGRITY

## enable-continuous-detection

**Description** Specifies whether continuous switching fabric testing, detection, and correction are enabled.

**Usage** Valid values are as follows. The recommended setting is yes for control modules and no for line interface modules (LIMs).

- yes—Enables continuous switching fabric testing, detection, and correction.
- no (the default)—Disables continuous switching fabric testing, detection, and correction.

**Example** set enable-continuous-detection = no

**Location** SYSTEM-INTEGRITY:integrity-config

## enable-core-dump

**Description** Enables or disables a core dump on system failure.

**Usage** Specify one of the following values:

- `yes`—Enables a core dump on system failure.
- `no`—Disables a core dump on system failure. This is the default value.

**Example** `set enable-core-dump = yes`

**Location** `DEBUG`

## enabled

**Description** Specifies whether a feature, interface, line, or test is enabled or disabled.

Following are the results of `enabled` settings in particular profiles:

- If `enabled` is set to `no` in the `ethernet` profile, packets routed to and received by the interface are discarded.
- When an OC3 interface is disabled, it transmits the OC3 idle signal to the remote end.
- In the `dns-local-table` subprofile of the `ip-global` profile, the `enabled` setting specifies whether the local Domain Name System (DNS) table in RAM is available when a DNS query fails:
  - If `enabled` is set to `no` (the default) and a DNS query times out, the request fails.
  - If `enabled` is set to `yes`, the Stinger unit attempts to resolve the query by using the host-to-address mapping in the DNS table in RAM. If the query has an entry in the table in RAM, the system returns the associated IP address(es) to the requester.
- If `enabled` is set to `yes` in the `continuity-config` or `loopback-config` subprofile of the `atm-oam` profile, the system resets the parameter to its `no` default when the continuity or loopback tests are complete.
- In the `remote-shelf-config` profile, the `enabled` setting causes a control link to be established between the host and the remote shelf.

**Usage** This parameter is set according to the profile that contains it.

- In all profiles except `sntp-info`, valid values are as follows:
  - `yes`—Enables the feature, interface, line, or test. This is the default for the `atm-internal` profile, `ethernet` profile, `snmp` profile, `tunnel-server` profile, `mp-options` subprofile, `ppp-answer` subprofile, and `ppp-options` subprofile.
  - `no`—Disables the feature, interface, line, or test. This is the default for all other profiles.

- Valid values for the sntp-info profile are as follows:
  - sntp-enabled—Specifies that the time is updated at each request to a server no matter what the time offset is between the Simple Network Time Protocol (SNTP) server and the Stinger unit.
  - sntp-passive—Specifies that an update occurs only when the update-threshold value has been reached.
  - sntp-disabled (the default)—Specifies that no updates occur.

**Example** set enabled = yes

**Location** ALARM

AL-DMT  
ANSWER-DEFAULTS:ppp-answer  
ATM-INTERNAL  
ATM-INTERNAL:traffic-shapers  
ATM-OAM:continuity-config  
ATM-OAM:loopback-config  
CONNECTION:mp-options  
CONNECTION:ppp-options  
DS1-ATM  
DS3-ATM  
DSL-THRESHOLD  
E3-ATM  
ETHERNET  
HDSL2  
IDSL:line-interface  
IP-GLOBAL:dns-local-table  
IP-GLOBAL:sntp-info  
OC3-ATM  
PRIVATE-ROUTE-TABLE  
REMOTE-SHELF-CONFIG  
SDSL  
SHDSL  
SNMP  
SYSTEM:traffic-shapers  
TERMINAL-SERVER  
TUNNEL-SERVER  
TUNNEL-SERVER:dialout-options  
VLAN-ETHERNET

enable-gdb

**Description** Enables or disables the GNU debugger (GDB).

**Usage** Specify one of the following values:

- yes—Enables the debugger on system failure.
- no—Disables the debugger on system failure. This is the default value.

**Example** set enable-GDB = yes

**Location** DEBUG

## enable-permit

**Description** Enables or disables control over telnet access to the system on the basis of the permit-list settings in the tac1 profile.

**Usage** Valid values are as follows:

- **yes**—Only the IP addresses specified in the permit-list subprofiles are allowed telnet access. Setting enable-permit to yes has no effect if none of the permit-list subprofiles have been configured.
- **no**—The permit-list settings have no effect. This is the default value.

**Example** set enable-permit = yes

**Location** TACL

## enable-vacm

**Description** Enables or disables the view-based access control model (VACM).

**Usage** Valid values are as follows:

- **yes**—Specifies that each object in each incoming Get, Set, GetNext, and GetBulk request, and each object in the sysTrapOID of each outgoing trap, is verified for VACM access.
- **no** (the default)—Disables VACM, enabling access to all objects in the system. However, security based on SNMPv1 community strings and the SNMP version 3 user-based security modem (SNMPv3 USM) is still used to determine access.

**Example** set enable-vacm = yes

**Location** SNMP

## encapsulation-protocol

**Description** Specifies the encapsulation method to use for a connection. Both sides of the connection must support the specified encapsulation method.

**Usage** Specify one of the following values:

- **mpp**—*Not supported.*
- **mp**—*Not supported.*
- **ppp**—Point-to-point protocol (PPP). Specify this value for PPP clients.
- **frame-relay**—Frame relay.
- **frame-relay-circuit**—Frame relay switching between interfaces.
- **tcp-raw**—*Not supported.*
- **atm**—Asynchronous Transfer Mode (ATM).
- **atm-frame-relay-circuit**—ATM-frame relay switching between interfaces.
- **atm-circuit**—ATM-to-ATM switching between interfaces.
- **atm-ima**—Inverse multiplexing over ATM (IMA) interfaces.

**Example** `set encapsulation-protocol = ppp`

**Location** CONNECTION

## encoding

**Description** Specifies the Asynchronous Transfer Mode (ATM) layer 1 line encoding used for the physical link(s).

**Usage** Valid values are as follows:

- `ami`—Specifies alternate mark inversion (AMI), a signaling method in which the 1 bits have alternating priority.
- `b8zs` (the default)—Specifies bipolar 8-zero substitution (B8ZS), an encoding method in which an alternating positive and negative voltage represents 1 (one), no voltage represents 0 (zero), and at least one bit out of every eight must be a 1.
- `hdb3`—Specifies high-density bipolar 3 (HDB3).

**Example** `set encoding = ami`

**Location** DS1-ATM:line-config

## end-of-packet-pattern

**Description** Specifies the pattern to be matched for end-of-packet detection.

**Usage** Specify a pattern end text of up to 64 characters.

**Example** `set end-of-packet-pattern = ##!`

**Dependencies** The `detect-end-of-pattern` parameter must be enabled for the `end-of-packet-pattern` parameter to take effect.

**Location** CONNECTION:tcp-clear-options

## end-port

**Dependencies** Specifies the last port to be isolated during an isolation or multiport tone test.

**Usage** Specify a port number between 1 and 72.

**Example** `set end-port = 3`

**Dependencies** This parameter is valid only if `specific-ports` is set to `no`.

**Location** LINE-TESTS

## enforce-address-security

**Description** Specifies whether the Stinger unit validates the IP address of an SNMP manager attempting to access the unit. If address security is not enforced, any SNMP manager that presents the appropriate community name is allowed in.

**Usage** Valid values are as follows:

- **yes**—Specifies that, before allowing access, the Stinger unit compares the source IP address of an SNMP manager to the host addresses specified by `read-access-hosts` and `write-access-hosts`. This is the default.
- **no**—Specifies that the Stinger unit does not compare IP addresses, but uses only the community name to validate SNMP access.

**Example** `set enforce-address-security = yes`

**Dependencies** The IP addresses in the `read-access-hosts` and `write-access-hosts` arrays do not restrict access unless `enforce-address-security` is set to `yes`.

**Location** `SNMP`

## enforce-password-check

**Description** Enables/disables password validation.

**Usage** Valid values are as follows:

- **yes**—Enables the system to validate that a password is unique and that it is at least 8 characters in length, with at least two numbers and four alphabetical characters.
- **no** (the default)—Disables password validation.

**Example** `set enforce-password-check = yes`

**Location** `USER`

## engine-boots

**Description** Read-only. Indicates the number of times that the SNMP agent on a Stinger unit has initialized itself since the SNMP `engine-id` value was last set.

**Usage** Read-only parameter with a value ranging from 0 to 4294967295.

**Example** `engine-boots = 12`

**Location** `SNMP`



## engine-id

**Description** Specifies an SNMP agents's administratively unique identifier.

**Usage** Specify a 12-byte hexadecimal value consisting of 24 hexadecimal digits. The default value is 0 (zero).

**Example** `set engine-id = 123456789abcdef0fedcba98`

**Location** SNMP

## error-averaging-period

**Description** Specifies the time period, in seconds, during which the system calculates the error-moving average for a modem on this line interface module (LIM), before the modem is considered to have failed.

**Usage** Specify a number in the range 1 through 512. The default value is 10 seconds.

**Example** `set error-averaging-period = 15`

**Dependencies** The operation of this parameter depends directly on the value of `error-threshold`.

**Location** LIM-SPARING-CONFIG:auto-lim-sparing-config:lim-sparing-config[n]

## error-count

**Description** Read-only. Indicates the number of errors experienced by each channel.

**Usage** The `error-count` value is read-only.

**Example** `error-count = 0`

**Location** ADSL-STAT  
IDSL-STAT  
SDSL-STAT  
T1-STAT

## errored-second

**Description** Indicates the number of 1-second intervals (out of a 15-minute sampling period) during which one or more cyclic redundancy check (CRC) anomalies are declared and/or one or more loss of synchronous word (LOSW) defects are declared.

**Usage** The `errored-second` value is read-only and helps you monitor interface operations.

**Example** `errored-second = 3`

**Location** HDLSL2-STAT:physical-statistic  
SHDSL-STAT:physical-statistic

## error-threshold

**Description** Specifies a threshold for errors in the following profiles:

- In the loopback-config subprofile of the atm-oam profile, error-threshold specifies the threshold for the number of loopback cells that can be lost. If the number of cells lost become equal to or greater than the value you specify, a trap is generated.
- In the lim-sparing-config[n] subprofile of the lim-sparing-config:auto-lim-sparing-config profile, error-threshold specifies the number of errors that must occur during the error-averaging period before a modem on this line interface module (LIM) is considered inoperable.

**Usage** Valid values are as follows:

- In loopback-config, specify a number from 0 through 10. The default is 0 (zero), which means that no trap is sent.
- In auto-lim-sparing-config, specify a number. The default value is 100.

**Example** set error-threshold = 5  
set error-threshold = 90

**Dependencies** In the auto-lim-sparing-config subprofile, an error-averaging-period value must be specified appropriately to make error-threshold usable.

**Location** ATM-OAM:loopback-config  
LIM-SPARING-CONFIG:auto-lim-sparing-config:lim-sparing-config[n]

## ether-if-type

**Description** Read-only. Indicates the type of physical Ethernet interface in use.

**Usage** The ether-if-type value is read-only. Valid values are as follows:

- utp—Indicates unshielded twisted pair (UTP), as specified in IEEE 802 (10BaseT) Ethernet.
- aui—Indicates an auxiliary unit interface (AUI) transceiver (thick Ethernet), as specified in IEEE 802.3 (10Base5) Ethernet.
- coax—Coaxial cable.

**Example** ether-if-type = utp

**Location** ETHERNET

## ethernet-type

**Description** Ethernet type.

**Usage** A two-byte hexadecimal number representing the Ethernet protocol. PPPoE values are 8863 (PPPoE Discovery Stage packets), and 8864 (PPP Session Stage packets). The system will forward or discard packets of the specified types, depending on how the filter is defined.

**Example** `set ethernet-type = 88:64`

**Location** `FLOW-SERVICES:flow-list [n]:layer2-classifier`

## event

**Description** Specifies an alarm event that triggers the actions indicated by the `action subprofile`.

**Usage** Valid values are as follows:

- `power-failure`—Specifies that the event is a redundant power supply failure.
- `fan-failure`—Specifies that the event is a redundant fan failure.
- `line-state-change` (the default)—Specifies that the event is a state change in a line.
- `slot-state-change`—Specifies that the event is a state change in a slot.
- `primary-switch-over`—Specifies that the event is a switchover of the primary control module functions to the secondary control module.
- `secondary-controller-state-change`—Specifies that the event is a state change in the secondary control module.
- `input-relay-closed`—Specifies that the event is the closure of an input relay-monitoring circuit.
- `input-relay-open`—Specifies that the event is the opening of an input relay-monitoring circuit.
- `low-temperature-trigger`—Specifies that the event is the crossing of a low-temperature threshold in the `thermal` profile.
- `high-temperature-trigger`—Specifies that that the event is the crossing of a high-temperature threshold in the `thermal` profile.

**Example** `set event = fan-failure`

**Location** `ALARM`

## event-overwrite-enabled

**Description** Specifies whether the system generates a trap when a new event has overwritten an unread event. Once sent, additional overwrites do not cause another trap to be sent until at least one table's worth of new events have occurred.

**Usage** Valid values are as follows:

- `yes`—Specifies that the system generates a trap when a new event has overwritten an unread event. This is the default.
- `no`—Specifies that the system does not generate a trap when a new event has overwritten an unread event.

**Example** `set event-overwrite-enabled = no`

**Location** `TRAP`

## `exact-match-call-routing`

**Description** Enables or disables the system's use of an exact match for call-route profile parameters when it selects devices.

**Usage** Valid values are as follows:

- `yes`—Specifies that the system searches for an exact match of call-route profile parameters when selecting devices.
- `no` (the default)—Specifies that the system does not search for an exact match of call-route profile parameters when selecting devices.

**Example** `set exact-match-call-routing = no`

**Location** `SYSTEM`

## `exclude-listed-commands`

**Description** Enable/disable permission for the users in the group to use the commands designated by the `command` parameter.

**Usage** Valid values are as follows:

- `yes`—Specifies that the users do not have permission to use the designated commands.
- `no` (the default)—Specifies that the users have permission to use the designated commands.

**Example** `set exclude-listed-commands = yes`

**Location** `USER-GROUP`

## `expect-callback`

**Description** *Not supported.* Specifies whether callback security is expected.

**Location** `CONNECTION:telco-options`

## `expected-far-end-frame-length`

**Description** Specifies the value of the far-end frame length expected during inverse multiplexing over ATM (IMA) group startup. If the actual frame length is not equal to `expected-far-end-frame-length`, IMA group startup is terminated.

**Usage** Valid values are as follows:

- `32`—IMA frame is 32 cells long.
- `64`—IMA frame is 64 cells long.
- `128`—IMA frame is 128 cells long. This is the default.
- `256`—IMA frame is 256 cells long.

**Example** `set expected-far-end-frame-length = 256`

**Dependencies** The parameter `far-end-check-frame-length` must be set to `yes` to enable the frame length check.

**Location** `IMAGROUP`

## `expected-far-end-ima-id`

**Description** Specifies a number to check against the inverse multiplexing over ATM (IMA) ID at the far end.

The far-end IMA ID is compared against this value during group startup. If the IDs do not match, the unit moves to the `ConfigAborted` state.

**Usage** Specify a number from 0 (zero) to 255.

**Example** `set expected-far-end-ima-id = 33`

**Dependencies** For this parameter to apply, `check-far-end-ima-id` must be set to `yes`.

**Location** `IMAGROUP`

## `external-change`

**Description** Read-only. Tracks the source of the most recent change to a profile.

**Usage** Read-only parameter with one of the following values:

- `yes`—Most recent read, create, or modify action on this profile was *not* performed using the command-line-interface.
- `no`—Most recent read, create, or modify action on this profile was performed using the command-line-interface.

**Example** `external-change = yes`

**Location** `ATM-QOS`  
`PNNI-METRICS`  
`PNNI-ROUTE-TNS`  
`PNNI-SUMMARY-ADDR`  
`ATM-SPVC-ADDR-CONFIG`  
`PNNI-IF-CONFIG`  
`PNNI-NODE-CONFIG`  
`PNNI-ROUTE-ADDR`

## external-fan-unit-failed

**Description** An alarm was received from the remote shelf fan to indicate a failure of the external fan unit.

**Usage** This parameter is read-only. Valid values are as follows:

- `yes`—An alarm was received.
- `no` (the default)—No alarms were received.

**Location** REMOTE-SHELF-STAT

## extra-traffic-flag

**Description** Read-only. Indicates whether extra traffic is being carried on the protection channel in automatic protection switching (APS).

**Usage** The `extra-traffic-flag` value is read-only. Valid values are as follows:

- `true`—Indicates that the protection channel is carrying extra traffic.
- `false`—Indicates that the protection channel is not carrying extra traffic..

**Example** `extra-traffic-flag = false`

**Location** APS-STAT

## ezd-error-count

**Description** Read-only. Number of times the system has detected excessive binary zeros that occurred since it was last reset.

**Usage** The `ezd-error-count` value is read-only.

**Example** `ezd-error-count = 47419`

**Location** DS3-ATM-STAT

E3-ATM-STAT

OC3-ATM-STAT

## F

### facility

**Description** Specifies the 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.

The facility value in the log profile affects all data streams. The facility 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.

**Usage** Valid values are as follows:

- local0 (the default)
- local1
- local2
- local3
- local4
- local5
- local6
- local7

**Example** `set facility = local4`

**Location** LOG

LOG:auxiliary-syslog:auxiliary-syslog[n]

### failure-notification-interval

**Description** Specifies the minimum interval between the sending of atmSoftPvcCallFailuresTrap notifications.

**Usage** Specify a value in the range from 0 to 3600 seconds. The default value is 30.

**Example** `set failure-notification-interval = 120`

**Location** ATM-SPVC-CONFIG

## failure-status

**Description** Read-only. Indicates the current failure status of the inverse multiplexing ATM (IMA) group, providing the reason why group traffic is in the DOWN state.

**Usage** The failure-status value is read-only. Valid values are as follows:

- no-failure—No failure of the IMA group. The unit is operational.
- start-up-ne—IMA group startup failure occurred at the near end.
- start-up-fe—IMA group startup failure occurred at the far end.
- failed-asymmetric-ne—IMA group startup failed due to asymmetry at the near end.
- failed-asymmetric-fe—IMA group startup failed due to asymmetry at the far end.
- insufficient-links-ne—IMA group startup failed due to insufficient links at the near end.
- insufficient-links-fe—IMA group startup failed due to insufficient links at the far end.
- blocked-ne—IMA group startup was blocked at the near end.
- blocked-fe—IMA group startup was blocked at the far end.
- other-failure—IMA group startup has some other failure.
- invalid-ima-version-ne—Near end reported an invalid IMA version.
- invalid-ima-version-fe—Far end reported an invalid IMA version.

**Example** failure-status = no-failure

**Location** IMA-GROUP-STAT

## failure-trap-enable

**Description** Enables or disables the generation of traps (notifications) in response to call failures.

**Usage** Specify one of the following values:

- yes—The system generates traps in response to call failures. This is the default value.
- no—The system does not generate traps in response to call failures.

**Example** set failure-trap-enable = no

**Location** ATM-SPVC-CONFIG



## far-end-check-frame-length

**Description** Enables or disables comparison of the actual far-end frame length with the `expected-far-end-frame-length` parameter during inverse multiplexing over ATM (IMA) group startup.

**Usage** Specify one of the following values:

- `yes`—Enables far-end frame length checking during IMA group startup.
- `no`—Disables far-end frame length checking during IMA group startup.

**Example** `set far-end-check-frame-length = yes`

**Location** `IMAGROUP`

## far-end-crc

**Description** Read-only. Indicates the number of cyclic redundancy check (CRC) errors detected by the ADSL transceiver unit (ATU) of the customer premises equipment (CPE).

**Usage** The `far-end-crc` value is read-only.

**Example** `far-end-crc = 0`

**Location** `AL-DMT-STAT:physical-statistic`

## far-end-db-attenuation

**Description** Read-only. Indicates the attenuation of the signal in decibels received from the customer premises equipment (CPE).

**Usage** The `far-end-db-attenuation` setting is read-only.

**Example** `far-end-db-attenuation = 0`

**Location** `SDSL-STAT:physical-statistic`

## far-end-fec

**Description** Read-only. Indicates the number of forward error correction (FEC) errors detected by the ADSL transceiver unit (ATU) on the customer premises equipment (CPE).

**Usage** The `far-end-fec` value is read-only.

**Example** `far-end-fec = 0`

**Location** `AL-DMT-STAT:physical-statistic`

## far-end-hec

**Description** Read-only. Indicates the number of header error control (HEC) errors detected by the ADSL transceiver unit (ATU) on the customer premises equipment (CPE).

**Usage** The far-end-hec value is read-only.

**Example** far-end-hec = 0

**Location** AL-DMT-STAT:physical-statistic

## far-end-ima-group-state

**Description** Read-only. Indicates the current operational state of the far-end inverse multiplexing over ATM (IMA) group.

**Usage** The far-end-ima-group-state value is read-only. Valid values are as follows:

- not-configured—IMA group is not configured.
- start-up—IMA group is in the startup state.
- start-up-ack—IMA group is in a transitional state and has transitioned out of IMA startup state.
- aborted-unsupported-framelength—IMA group connection failed because the Frame length (M) received from the remote end was not acceptable to the local end.
- aborted-incompatible-symmetry—IMA group connection failed because the remote end and local end have incompatible group symmetry modes.
- aborted-other—IMA group connection failed for some other reasons.
- insufficient-links—IMA group connection is currently in the insufficient links state.
- blocked—IMA group connection is in the blocked state.
- operational—IMA group connection is in the operational state.
- aborted-unsupported-version—Stinger unit moved to the configAborted state because of an IMA version mismatch between the local and remote ends.

**Example** far-end-ima-group-state = operational

**Location** IMA-GROUP-STAT:ima-rt

## far-end-num-failures

**Description** Read-only. Indicates the number of times a far-end group failure (for example, configAborted or insufficient links) has been reported in the current 15-minutes interval.

**Usage** The far-end-num-failures value is read-only. Valid values range from 0 ((zero) to 2147483647.

**Example** far-end-num-failures = 6

**Location** IMA-GROUP-STAT:ima-group-statistic

## far-end-rx-failure-status

**Description** Read-only. Indicates the far end receive (RX) failure status of the IMA link.

**Usage** Valid values for this read-only parameter are as follows:

- no-failure—IMA link does not have any failure.
- ima-link-failure—IMA link experienced a failure at the IMA layer.
- lif-failure—IMA link experienced a loss of IMA frame (LIF) failure.
- lods-failure—IMA link experienced a loss of delay synchronization (LODS) failure.
- misconnected—IMA link is misconnected to the far-end.
- blocked—IMA link is in blocked state.
- fault—IMA link is in fault state.
- far-end-tx-link-unusable—Far end transmit of the IMA link is in an unusable state.
- far-end-rx-link-unusable—Far end receive of the IMA link is in an unusable state.

**Example** far-end-rx-failure-status = no-failure

**Location** DS1-ATM-STAT:ima-link-status

## far-end-rx-link-state

**Description** Read-only. Indicates the far-end receive (RX) state of the DS1-ATM link.

**Usage** Valid values for this read-only parameter are as follows:

- unusable-no-given-reason—IMA link is not usable but the reason is not known.
- unusable-fault—IMA link is not usable because of a fault.
- unusable-misconnected—IMA link is not usable because it is misconnected with the far end.
- unusable-inhibited—IMA link is not usable because it is in an inhibited state.
- unusable-failed—IMA link is not usable because it is in failed state.
- usable— IMA link is usable.
- active—IMA link is active, part of an IMA group, and carrying traffic from the ATM layer.

**Example** far-end-rx-link-state = not-in-group

**Location** DS1-ATM-STAT:ima-link-status

## far-end-rx-num-failures-counter

**Description** Read-only. Indicates the number of times a far-end (FE) receive failure alarm condition has been entered on the Rx-Unusable-FE link. This is an optional attribute.

**Usage** Valid for this read-only parameter range from 0 (zero) to 2147483647.

**Example** far-end-rx-num-failures-counter = 0

**Location** DS1-ATM-STAT:ima-link-statistic

## far-end-rx-unusable-secs-counter

**Description** Read-only. Indicates the count of seconds with receive (RX) unusable indications at the far-end link.

**Usage** The valid range for this read-only parameter is from 0 (zero) to 2147483647.

**Example** far-end-rx-unusable-secs-counter = 134

**Location** DS1-ATM-STAT:ima-link-statistic

## far-end-sev-errored-secs-counter

**Description** Read-only. Indicates the count of one second intervals containing one or more remote defect indicator (RDI) defects in inverse multiplexing over ATM (IMA), except during the unavailable seconds for IMA far end (UAS-IMA-FE) condition.

**Usage** The valid range for this read-only parameter is from 0 (zero) to 2147483647.

**Example** far-end-sev-errored-secs-counter = 0

**Location** DS1-ATM-STAT:ima-link-statistic

## far-end-txclock-mode

**Description** Read-only. Indicates the transmit clocking mode used by the far-end inverse multiplexing over ATM (IMA) group.

**Usage** Valid values for this read-only parameter are as follows

- ctc—Common transmit clock. The transmit clocks of the links within the IMA group are derived from the same clock source.
- itc—Independent transmit clock. The transmit clocks of the links within the IMA group are derived from their respective receive clocks.

**Example** far-end-txclock-mode = ctc

**Location** IMA-GROUP-STAT

## far-end-tx-link-state

**Description** Read-only. Indicates the transmit state of the link.

**Usage** Valid values for this read-only parameter are as follows

- not-in-group—IMA link is not part of an IMA group.
- unusable-no-given-reason—IMA link is not usable, but the reason is not known.
- unusable-fault—IMA link is not usable because of a fault.
- unusable-misconnected—IMA link is not usable because it is misconnected with the far end.
- unusable-inhibited—IMA link is not usable because it is in an inhibited state.
- unusable-failed—IMA link is not usable because it is in failed state.
- usable—IMA link is usable.
- active—IMA link is active, part of an IMA group, and carrying traffic from the ATM layer.

**Example** far-end-tx-link-state = not-in-group

**Location** DS1-ATM-STAT:ima-link-status

## far-end-tx-num-failures-counter

**Description** Read-only. Indicates the number of times a far-end (FE) transmit (TX) failure alarm condition has been entered on the Tx-Unusable-FE link. This is an optional attribute.

**Usage** The valid range for this read-only parameter is from 0 (zero) to 2147483647.

**Example** far-end-tx-num-failures-counter = 12

**Location** DS1-ATM-STAT:ima-link-statistic

## far-end-tx-unusable-secs-counter

**Description** Read-only. Indicates the count of seconds with Tx Unusable indications from the far-end transmit (TX) link.

**Usage** The valid range for this read-only parameter is from 0 (zero) to 2147483647.

**Example** far-end-tx-unusable-secs-counter = 0

**Location** DS1-ATM-STAT:ima-link-statistic

## far-end-unavail-secs-counter

**Description** Read-only. Indicates the count of unavailable seconds at the far end.

Unavailability begins at the onset of 10 contiguous severely errored seconds for inverse multiplexing over ATM (SES-IMA-FE) and ends at the onset of 10 contiguous seconds with no SES-IMA-FE.

**Usage** Valid range for this read-only parameter is from 0 (zero) to 2147483647.

**Example** far-end-unavail-secs-counter = 0

**Location** DS1-ATM-STAT:ima-link-statistic

## fault-clearing-time

**Description** Specifies the amount of time, in seconds, after which a fault on an inverse multiplexing over ATM (IMA) link is cleared.

**Usage** Valid range is 0 (zero) to 2147483647.

**Example** set fault-clearing-time = 10

**Dependencies** For fault-clearing-time to apply, fault-clearing-type must be set to auto.

**Location** DS1-ATM:line-config:ima-option-config:rx-link-config  
DS1-ATM:line-config:ima-option-config:tx-link-config

## fault-clearing-type

**Description** Specifies whether fault clearing on an inverse multiplexing over ATM (IMA) link is automatic or manual.

**Usage** Valid values are as follows:

- manual—Link fault clearing is manual. Any fault is permanent until cleared by the user.
- auto—Link fault clearing is automatic. A fault is automatically cleared after the user-defined time. This is the default.

**Example** set fault-clearing-type = auto

**Location** DS1-ATM:line-config:ima-option-config:rx-link-config  
DS1-ATM:line-config:ima-option-config:tx-link-config

## f-bit-error-count

**Description** Read-only. Indicates the number of framing bit errors received since the last time the unit was reset.

**Usage** This read-only display is used for monitoring line communications as follows:

- For the ds3-atm-stat profile—If three or more errors occur in up to 16 consecutive framing bits in a DS3 M-frame, a DS3 out-of-frame defect is detected. If an out-of-frame defect is consistent for up to 10 seconds, a DS3 loss-of-frame defect is detected.
- For the e3-atm-stat profile—Number of F-bit errors. If three or more errors occur in up to 16 consecutive F-bits in an E3 M-frame, an E3 out-of-frame defect is detected. If an out-of-frame defect is consistent for up to 10 seconds, an E3 loss-of-frame is detected.

**Example** f-bit-error-count = 0

**Location** DS3-ATM-STAT  
E3-ATM-STAT

## fbm-dbm-mode

**Description** For Annex C line interface modules (LIMs) only, specifies the bit-map mode for a line.

**Usage** Valid values are as follows:

- fbm (the default)—Specifies fixed bit-map mode.
- dbm—Specifies dual bit-map mode.

**Example** set fbm-dbm-mode = dbm

**Location** AL-DMT:line-config

## fc1loc-gauge

**Description** Specifies the gauge of the cable in the loop of a copper loop test (CLT).

**Usage** Valid values are as follows:

- If you have selected English units, enter one of the following American wire gauge (AWG) values:
  - 22
  - 24
  - 26
- If you have selected metric units, enter one of the following values to specify a gauge in tenths of a millimeter:
  - 4
  - 5
  - 6

**Example** When metric units have been selected, the following example specifies a cable loop of 0.4mm:

```
set fciloc-gauge = 4
```

**Dependencies** For `fciloc-gauge` to apply, you must specify the appropriate unit of measurement in `fciloc-unit`.

**Location** CLT-COMMAND

## fciloc-unit

**Description** Specifies the units of measurement used for a first coil location test in a copper loop test (CLT).

**Usage** Valid values are as follows:

- `english`—Specifies that English units are used for the measurement.
- `metric` (the default)—Specifies that metric units are used for the measurement.

**Example** `set fciloc-unit = metric`

**Location** CLT-COMMAND

## fdl

**Description** Specifies the Facilities Data Link (FDL) protocol that the telephone company uses to monitor the quality and performance of a T1 line. The protocol provides information at regular intervals to your carrier's maintenance requirements.

**Usage** Specify one of the following values:

- `none`—Disables FDL signaling. This is the default.
- `AT&T`—Specifies AT&T FDL signaling
- `ANSI`—Specifies ANSI FDL signaling
- `sprint`—Specifies Sprint FDL signaling



**Note** Currently the `sprint` setting conforms to the same functionality as the `at&t` setting.

**Example** `set fdl = at&t`

**Dependencies** FDL does not apply to D4 framed lines. However, even if you do not choose the FDL protocol, the Stinger unit accumulates D4 and ESF performance statistics in the FDL Statistics windows.

**Location** DS1-ATM:line-config

## feb-error-count

**Description** Read-only. Indicates the number of far-end block errors (C-bit coding violations) received since the last time the unit was reset.

**Usage** The `feb-error-count` value is read-only.



**Example** `feb-error-count = 0`

**Location** DS3-ATM-STAT  
E3-ATM-STAT

## `fepl-failure`

**Description** Read-only. Indicates whether a far-end protection line (FEPL) failure has occurred.

**Usage** Valid values for this read-only parameter are as follows:

- `true`—Indicates a FEPL failure.
- `false`—Indicates no FEPL failure has occurred.

**Example** `fepl failure = false`

**Location** APS-STAT

## `fepl-mismatch-clear-timer-duration`

**Description** Specifies the duration of the clear timer for a far-end protection line (FEPL) mismatch, in tenths of milliseconds. This setting is part of the automatic protection switching (APS) system.

**Usage** Specify a number from 0 through 4,294,967,295. The default is 1000.

**Example** `set fepl-mismatch-clear-timer-duration = 2000`

**Location** APS-CONFIG

## `fepl-mismatch-failure-timer-duration`

**Description** Specifies the time duration allowed for a far-end protection line (FEPL) failure mismatch, in tens of milliseconds.

**Usage** Specify a number from 0 through 4,294,967,295. The default is 250.

**Example** `set fepl-mismatch-failure-timer-duration = 300`

**Location** APS-CONFIG

## `fifo-overflow-counter`

**Description** Read-only. Indicates the number of cells dropped due to first-in-first-out (FIFO) overflow.

**Usage** The `fifo-overflow-counter` value is read-only.

**Example** `fifo-overflow-counter = 0`

**Location** OC3-ATM-STAT

## filter-name

**Description** Specifies the name of a filter.

- In a filter profile, the name you assign becomes the filter profile's index, which is used to apply the filter to interfaces.
- In an ethernet profile, the name specifies a data filter to apply to the Ethernet interface.

**Usage** Specify a filter name of up to 36 characters. The default is null.

**Example** `set filter-name = ip-spoof`

**Location** `ETHERNET`  
`FILTER`

## filter-persistence

**Description** Enables or disables filter persistence across connection state changes.

A state change occurs when a connection temporarily stops operating because of inactivity on the line.

**Usage** Valid values are as follows:

- `yes`—Filters persist across state changes.
- `no` (the default)—Filters do not persist across state changes.

**Example** `set filter-persistence = yes`

**Location** `ANSWER-DEFAULTS:session-info`  
`CONNECTION:session-options`

## filter-required

**Description** Specifies whether access to the filter is required to establish the session.

In the answer-defaults profile, this parameter is used for RADIUS user profiles that apply a filter and do not specify a value for `Ascend-Filter-Required` (50).

**Usage** Valid values are as follows:

- `yes`—Disconnects the call with cause code 425 if the filter is not found locally or in RADIUS.
- `no` (the default)—Establishes the session even if the specified filter is not found, and logs a notice-level message.

**Example** `set filter-required = yes`

**Dependencies** This setting does not apply if the profile does not specify a filter by name.

**Location** `ANSWER-DEFAULTS:session-info`  
`CONNECTION:session-options`

## filter-type

**Description** Type of multicast group address filtering.

**Usage** Allowable values are:

- **exclusive**—Access to all multicast group addresses except those listed in the filter-list is allowed.
- **inclusive**—Access only to those multicast group addresses listed in the filter-list is allowed.
- **none** (the default)—Access to all multicast groups is allowed.

**Example** set filter-type = inclusive

**Location** MCAST-SERVICE

## finger

**Description** Enables or disables response to remote finger queries.

The finger facility is described in RFC 1288. The finger forwarding service, which uses the hostname format *@host1@host2*, is not supported. If the remote client uses the forwarding request format, the system sends a message that the service is denied.

**Usage** Valid values are as follows:

- **yes**—Accepts finger queries and returns the requested active session details to a remote client. The client can ask for short or wide format of session information, and can request the details of all sessions, or of a single session.
- **no** (the default)—Rejects queries from finger clients and sends a message that the finger online user list is denied.

**Example** set finger = yes

**Location** IP-GLOBAL

## firmware-startup-stage

**Description** Read-only. Indicates the current firmware state.

**Usage** The firmware-startup-stage value is read-only.

**Example** firmware-startup-stage = idle

**Location** SDSL-STAT:physical-statistic

## firmware-ver

**Description** Read-only. Indicates the version number of the line interface module (LIM) firmware.

**Usage** The firmware-ver value is read-only.

**Example** `firmware-ver = 1.4.1`

**Location** `AL-DMT-STAT:physical-status`  
`HDSL2-STAT:physical-status`  
`SHDSL-STAT:physical-status`

## `first-coil-location`

**Description** Specifies the distance to the first load coil detected in a copper loop test (CLT).

**Usage** Distance is reported in centimeters if `fcloc-unit` is set to `metric`. Distance is reported in hundredths of feet if `fcloc-unit` is set to `English`. A value of 0 indicates no load coil was detected.

**Example** `first-coil-location = 74`

**Location** `CLT-RESULT`

## `first-level-user`

**Description** Name of a first-level user profile. The default setting is `null`.

**Usage** Specify the name of a valid user profile.

**Example** `set first-level-user = john`

**Location** `USER`

## `first-retry-timer`

**Description** Specifies the initial interval, in milliseconds, that the system waits before retransmitting control packets in the attempt to establish a Layer 2 Tunneling Protocol (L2TP) tunnel with an L2TP network server (LNS) system.

**Usage** Enter a number from 100 to 5000. The default is 1000.

**Example** `set first-retry-timer = 1000`

**Dependencies** This timer works with the `retry-count` parameter in establishing and maintaining tunnel sessions.

**Location** `L2-TUNNEL-GLOBAL:l2tp-config`

## `flow-control`

**Description** Specifies the flow control method used on the serial port.

**Usage** Valid values are as follows:

- `none` (the default)—Specifies no flow control.
- `xon-xoff`—Specifies software flow control.
- `hardware-handshake`—Specifies hardware flow control.

**Example** `set flow-control = xon-xoff`

**Location** SERIAL

## flow-services

**Description** Name of a flow-services profile that defines the proper VLAN tag mapping for this connection.

**Usage** The name of a valid flow-services profile.

**Example** `set flow-services = enterprisel-vlans`

**Location** CONNECTION:session-options

## force-56kbps

**Description** *Not supported.* Specifies whether to use only the 56Kbps portion of a channel, even when all 64Kbps appear to be available.

**Location** ANSWER-DEFAULTS  
CALL-INFO  
CONNECTION:telco-options

## force-fragmentation

**Description** Enables or disables the fragmentation of packets with the DF (Don't Fragment) bit set, sent by client software.

If outdated client software sends large packets with the DF bit set, you can set this parameter to force the system to fragment the packets anyway.

**Usage** Valid values are as follows:

- **yes**—Forces prefragmentation of large IP frames before they are sent to the remote agent, even if the frame has the DF bit set. This behavior is not standard and prevents maximum transmission unit (MTU) discovery mechanisms.
- **no**—Sends an Internet Control Message Protocol (ICMP) message if a frame needs fragmentation and the DF bit is set. This is the default.

**Example** `set force-fragmentation = no`

**Location** ATMP

## forward

**Description** Specifies the forwarding action of a filter:

- For a data filter, the forwarding action determines whether the system forwards or discards packets that match the filter specification.
- For a call filter, the forwarding action determines whether matching packets reset the session timer.

**Usage** Valid values are as follows. When no filters are in use, the system forwards all packets by default. When a filter is in use, the default is to discard matching packets.

- `yes`—Forwards packets that match the filter rules.
- `no`—Discards packets that match the filter rules. This is the default.

**Example** `set forward = yes`

**Dependencies** This setting has no effect on route filters or type-of-service (TOS) filters.

**Location** `FILTER:input-filters[n]`  
`FILTER:output-filters[n]`

## fr-08-mode

**Description** Specifies how frame relay packet headers are processed when they flow between the frame relay interface and the Asynchronous Transfer Mode (ATM) interface.



**Note** This parameter is not currently used in the `atm-connect-options` subprofile.

**Usage** Valid values are as follows:

- `translation`—RFC 1490 headers are converted to RFC 2684 header format. This is the default.
- `transparent`—RFC 1490 headers are not converted to RFC 2684 header format.

**Example** `set fr-08-mode = transparent`

**Location** `CONNECTION:atm-connect-options`  
`CONNECTION:atm-options`

## framed-only

**Description** Specifies whether an incoming call must use a framed protocol or not.

**Usage** Valid values are as follows:

- `yes`—Specifies that an incoming call must use a framed protocol.
- `no`—Specifies that an incoming call need not use a framed protocol. This is the default.

**Example** `set framed-only = yes`

**Location** `CONNECTION`

## frame-length

**Description** Specifies the frame length for an inverse multiplexing ATM (IMA) group.

**Usage** Valid values are as follows:

- 32—IMA frame is 32 cells long.
- 64—IMA frame is 64 cells long.
- 128—IMA frame is 128 cells long. This is the default.
- 256—IMA frame is 256 cells long.

**Example** `set frame-length = 64`

**Location** IMAGROUP

## framer-mode

**Description** Specifies the Asynchronous Transfer Mode (ATM) framer mode for DS3 and E3 interfaces. Specifies the SONET mode for OC3 interfaces.

**Usage** Valid values are as follows:

- For DS3-ATM interfaces:
  - `c-bit-adm`—Free-running and fixed-stuffing C-bit ATM direct-mapping (ADM) mode.
  - `c-bit-plcp`—Free-running and fixed-stuffing C-bit Physical Layer Convergence Protocol (PLCP) mode. This is the default.
  - `c-bit-adm-loop-timed`—Loop-timed C-bit ADM mode.
  - `c-bit-plcp-loop-timed`—Loop-timed C-bit PLCP mode.
  - `c-bit-adm-frame-locked`—Frame-locked C-bit ADM mode.
  - `c-bit-plcp-frame-locked`—Frame-locked C-bit PLCP mode.
- For E3-ATM interfaces:
  - `g832-adm`—G.832 framing, ADM, fixed-stuffing mode.
  - `g832-adm-frame-locked`—Frame-locked E3-ATM G.832 ADM mode.
  - `g832-adm-loop-timed`—Loop-timed E3-ATM G.832 ADM mode.
- For OC3-ATM interfaces:
  - `sonet`—Synchronous Optical Network mode.
  - `sdh`—Synchronous digital hierarchy mode.

**Example** `set framer-mode = c-bit-plcp-frame-locked`

**Location** DS3-ATM:line-config  
E3-ATM:line-config  
OC3-ATM:line-config

## framer-rate

**Description** Specifies the framing to use on the line.

**Usage** Currently, the only supported value is `sts-3c`, which is used for a 155.52Mbps interface in the U.S. as well as the equivalent European 155Mbps interface (STM-1).

**Example** `set framer-rate = sts-3c`

**Location** `OC3-ATM:line-config`

## frame-relay-enabled

**Description** Read-only. Indicates whether frame relay is enabled on the Stinger unit.

**Usage** The `frame-relay-enabled` value is read-only and can have one of the following settings:

- `yes`—Indicates that frame relay is enabled.
- `no`—Indicates that frame relay is not enabled.

**Example** `frame-relay-enabled = no`

**Location** `BASE`

## frame-relay-profile

**Description** Specifies the name of the `frame-relay` profile to use.

**Usage** Specify the name of a `frame-relay` profile, exactly as specified by the `fr-name` value, including case changes.

**Example** `set frame-relay-profile = att-dce`

**Dependencies** For `frame-relay-profile` to apply, you must set `fr-direct-enabled` to `no`.

**Location** `CONNECTION:fr-options`



## framer-sync-status

**Description** Read-only. Indicates the state of the HDSL2 framer. Provides troubleshooting information and can assist in determining the reason for a loss-of-signal (LOS) condition.

**Usage** Valid values for this read-only parameter are as follows:

- in-sync—Framer is in synchronization. The HDSL2 framers are successfully passing HDSL2 frames.
- resync-state 1 through resync-state 5—HDSL2 framer is trying to regain synchronization.
- out-of-sync—HDSL2 framer is out of synchronization and is not trying to regain synchronization.
- out-of-sync-pre-sync—HDSL2 framer is out of synchronization and is not trying to gain synchronization.

**Example** `framer-sync-status = in-sync`

**Location** HDSL2-STAT:physical-statistic  
SHDSL-STAT:physical-statistic

## frame-type

**Description** *Not currently used.* Specifies the super-framing mode used for the physical link(s).

**Usage** Valid values are as follows:

- d4—Fourth-generation channel bank
- esf—Extended Super Frame format, a T1 format that uses the framing bit for nonintrusive signaling and control. This is the default.
- 703

**Example** `set frame-type = esf`

**Location** DS1-ATM:line-config

## fr-answer

**Description** Specifies whether the Stinger unit answers incoming connections that use frame relay encapsulation.

**Usage** Valid values are as follows:

- yes—Specifies that the Stinger unit answers incoming connections that use frame relay encapsulation. This is the default.
- no—Specifies that this function is disabled.

**Example** `fr-answer = yes`

**Location** ANSWER-DEFAULTS

**fr-direct-dlci**

**Description** *Not currently used.* Specifies the data link connection identifier (DLCI) of the frame relay direct connection.

**Usage** Specify a number from 16 through 91.

**Example** `set fr-dlci = 16`

**Location** CONNECTION:fr-options

**fr-direct-enabled**

**Description** *Not currently used.* Specifies that the Stinger unit uses the connection for Frame Relay Direct.

**Usage** Valid values are as follows:

- **yes**—Specifies that the Stinger unit uses the connection for frame relay direct.
- **no**—Specifies that the Stinger unit does not use the connection for frame relay direct. This is the default

**Example** `set fr-direct-enabled = yes`

**Dependencies** If encapsulation-protocol is set to frame-relay or frame-relay-circuit, fr-direct-enabled does not apply.

**Location** CONNECTION:fr-options

**fr-direct-profile**

**Description** *Not currently used.* Specifies the name of the frame relay profile to be used for frame relay direct routing

**Usage** Specify a name of up to 16 characters.

**Example** `set fr-direct-profile = cingula`

**Location** CONNECTION:fr-options

**frdl**

**Description** Specifies the password for the frame relay pseudo user.

**Usage** Specify a password of up to 21 characters.

**Example** `set frdl = yourpass`

**Location** EXTERNAL-AUTH:password-profile

## fr-dlci

**Description** Specifies a frame relay data link connection identifier (DLCI) number to use for frame relay direct connections.

**Usage** Specify the DLCI obtained from the frame relay administrator for frame relay direct links. The default is null. More than one direct PPP connection can share an fr-dlci number.

**Example** set fr-dlci = 72

**Dependencies** If fr-direct-enabled is set to no, fr-dlci does not apply. The fr-dlci parameter does not apply to gateway or circuit connections.

**Location** CONNECTION:fr-options

## frequency-justification-count

**Description** Read-only. Indicates the count of frequency justification instances that have taken place.

These operations monitor and reinforce synchronicity in the sending of packets.

**Usage** The frequency-justification-count value is read-only.

**Example** frequency-justification-count = 0

**Location** OC3-ATM-STAT

## fr-linkdown-enabled

**Description** Specifies whether a trap (notification) is sent whenever a data link connection identifier (DLCI) is brought down.

**Usage** Valid values are as follows:

- yes—Specifies that a trap is sent whenever a DLCI is brought down. This is the default.
- yes—Specifies that a trap is not sent whenever a DLCI is brought down.

**Example** set fr-linkdown-enabled = no

**Dependencies** If you set fr-linkdown-enabled to yes, you must also set alarm-enabled to yes for a trap to be sent whenever a DLCI is brought down.

**Location** TRAP

## fr-link-type

**Description** *Not used.* Specifies the type of link for the circuit end point.

**Usage** Valid values are as follows:

- `transparent-link`—Specifies a 1:1 circuit. It requires two end points that specify the same circuit name and the transparent-link type. If only one end point is specified, data received on the specified DLCI is dropped. If more than two transparent-link end points are specified with the same circuit name, only two of the profiles will be used to form a circuit. This is the default.
- `host-link`—Specifies virtual channel trunking with multiple end points on the host side.
- `trunk-link`—Specifies virtual channel trunking with a single end point on the trunk side.

**Example** `set fr-link-type = transparent-link`

**Location** CONNECTION:fr-options  
FRDLCI-STAT:dlci-ident  
FRPVC-STAT:dlci-members [n]

## fr-linkup-enabled

**Description** Specifies whether a trap (notification) is sent whenever a data link connection identifier (DLCI) is brought up.

**Usage** Valid values are as follows:

- `yes`—Specifies that a trap is sent whenever a DLCI is brought up. This is the default.
- `no`—Specifies that a trap is not sent whenever a DLCI is brought up.

**Example** `set fr-linkup-enabled = no`

**Dependencies** If you set `fr-linkup-enabled` to `yes`, you must also set `alarm-enabled` to `yes` for a trap to be sent whenever a DLCI is brought up.

**Location** TRAP

## fr-name

**Description** Specifies the name of a frame-relay profile.

**Usage** Specify a unique of no more than 15 characters. The default is null.

**Example** `set fr-name = att-dce`

**Location** FRAME-RELAY

## front-end-type

**Description** Specifies the front-end type of the transceiver: a long-haul or short-haul line interface unit.

**Usage** Valid values are as follows:

- `short-haul`—Sets the port for short-haul mode, which sets the receive sensitivity to -12dB in E1 mode and -30dB in T1 mode. A cross-connect receives a cell stream on one interface and transmits it on another. This is the default.
- `long-haul`—Sets the port to the long-haul mode, which sets the receive sensitivity on the interface to -43dB in E1 mode and -36dB in T1 mode.

**Example** `set front-end-type = short-haul`

**Dependencies** Consider the following:

- For the `short-haul` setting to apply, you must also set the `line-length` parameter to the length of the cable that connects to the digital cross-connect.
- For the `long-haul` setting to apply, you must also specify the correct value for the `line-build-out` parameter.
- The `long-haul` setting requires 120-ohm termination.

**Location** `DS1-ATM:line-config`

## fr-profile

**Description** Specifies or indicates, according to the profile, the name of the frame-relay profile to use for a frame relay direct connection.

**Usage** Valid values are as follows:

- In a `fr-options` subprofile, specify the name of a configured frame-relay profile, exactly as specified by the `fr-name` setting, including case changes.
- In a `dlci-ident` subprofile, a read-only value specifying the frame-relay profile over which the DLCI is established.
- In a `dlci-members [n]` subprofile, a read-only value specifying the frame-relay profile over which the DLCI is established.

**Example** `set fr-profile = att-dce`

**Dependencies** For `fr-profile` to apply, you must set `fr-direct-enabled` to `yes`. The `fr-profile` parameter does not apply to gateway or circuit connections.

**Location** `CONNECTION:fr-options`  
`FRDLCCI-STAT:dlci-ident`  
`FRPVC-STAT:dlci-members [n]`

### ft1-caller

**Description** *Not supported.* Specifies whether the system allows fractional T1 dial-out.

**Location** CALL-INFO  
CONNECTION:telco-options

### function

**Description** Read-only. Indicates the current function of the controller in this context.

**Usage** Read-only parameter with the following possible values:

- no-function
- primary
- secondary

**Example** function = secondary

**Location** REDUNDANCY-STATS:context-stats

## G

### gain-default

**Description** Specifies the default gain value in decibels (dB) for automatic gain control (AGC).

**Usage** Valid values are as follows:

- 16—Specifies 16dB, the optimum for upstream transmission.
- 20—Specifies 20dB, the optimum value for downstream transmission.

**Example** `set gain-default = 20`

**Location** `AL-DMT:fast-path-config`

### gamma-ima-value

**Description** Specifies the number of consecutive valid inverse multiplexing over ATM (IMA) Control Protocol (ICP) cells that must be detected before the system moves to IMA SYNC state from the PRESYNC state.

**Usage** Specify a number from 1 to 5.

**Example** `set gamma-ima-value = 1`

**Location** `IMAHW-CONFIG`

### gateway-address

**Description** Specifies the IP address of a next-hop router used to reach the destination address specified by a static or private route. A next-hop router is directly connected to the same Ethernet segment as the Stinger unit, or is one hop away on a WAN link.

**Usage** Specify an IP address. The default is 0.0.0.0.

**Example** `set gateway-address = 2.2.2.2`

**Location** `IP-ROUTE`  
`PRIVATE-ROUTE-TABLE:route-description-list [n]`

### gdb-host

**Description** Specifies the name or IP address of the host running GNU debugger (GDB).

**Usage** Specify an alphanumeric value up to 31 characters long. The default is blank.

**Example** `set gdb-host = GNUs new`

**Location** `DEBUG`

## generic-field

**Description** Specifies a field used as a generic bit mask stored in nonvolatile memory and preserved over resets and power downs.

**Usage** Specify a numeric value ranging from 0 to 4294967295.

**Example** `set generic-field = 123456`

**Location** `DEBUG`

## glite-atm-48

**Description** Specifies whether code images for ADSL 48-port G.lite line interface modules (LIMs) are to be stored in flash memory.

**Usage** Valid values are as follows:

- `auto`—Causes the system to load images for ADSL 48-port G.lite LIMs that are installed in the Stinger unit, and to skip images for modules that are not installed. This is the default.
- `load`—Causes the system to load the image, even if no ADSL 48-Port G.lite LIMs are installed.
- `skip`—Causes the system to skip the image, even if an ADSL 48-Port G.lite LIM is installed.



**Note** A module is considered present in the system if a `slot-type` profile exists for that module type. The system creates a `slot-type` profile when it first detects the presence of a module, and does not delete the profile unless you use the `slot -r` command to permanently remove a module that is no longer installed in the system, or clear nonvolatile RAM (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.

**Example** `set glite-atm-48 = auto`

**Location** `LOAD-SELECT`

## global

**Description** *Not used.* Specifies the highest level of the Private Network-to-Network Interface (PNNI) hierarchy that lies within the global scope.

**Usage** Specify a number from 0 to 104. The default value is 0.

**Location** `PNNI-NODE-CONFIG:node-scope-mapping`



## global-vrouter

**Description** Specifies the name of the global virtual router (the main router).

**Usage** Specify up to 23 characters. The default is main.

**Example** `set global-vrouter = test`

**Location** IP-GLOBAL

## gmt-offset

**Description** Specifies the local time zone as an offset from the Coordinated Universal Time (UTC).

When Simple Network Time Protocol (SNTP) has been enabled, specifying the time zone allows the system to query the server to maintain its system time.

**Usage** Because UTC is in the same time zone as Greenwich Mean Time (GMT), specify the offset in hours, using a 24-hour clock. Because some time zones, such as Newfoundland, cannot use an even-hour boundary, the offset includes 4 digits and is specified in half-hour increments. Valid values are as follows:

```
utc-1130
utc-1100
utc-1030
utc-1000
utc-0930
utc-0900
utc-0830
utc-0800
utc-0730
utc-0700
utc-0630
utc-0600
utc-0530
utc-0500
utc-0430
utc-0400
utc-0330
utc-0300
utc-0230
utc-0200
utc-0130
utc-0100
utc-0030
utc+0000 (the default)
utc+0030
utc+0100
utc+0130
utc+0200
utc+0230
utc+0300
utc+0330
```

utc+0400  
utc+0430  
utc+0500  
utc+0530  
utc+0600  
utc+0630  
utc+0700  
utc+0730  
utc+0800  
utc+0830  
utc+0900  
utc+0930  
utc+1000  
utc+1030  
utc+1100  
utc+1130  
utc+1200

**Example** Use the following examples to help you set `gmt-offset`:

- To set the offset for Newfoundland, which is 1.5 hours ahead of UTC:  
`set gmt-offset = utc+0130`
- To set the offset for San Francisco, which is 8 hours ahead of UTC:  
`set gmt-offset = utc+0800`
- To set the offset for Frankfurt, which is 1 hour behind UTC:  
`set gmt-offset = utc-0100`

**Location** IP-GLOBAL:sntp-info

## *group-address*

**Description** A multicast group address (a class D IP address). You can specify a full group address or a group range. If you specify a prefix (such as /8 in the value 226.0.0.0/8), the system automatically updates the `group-mask` parameter with the appropriate decimal value (such as 255.0.0.0).

**Usage** Specify an IP address in dotted decimal notation.

**Example** `set group-address = 231.1.1.1`

**Dependencies** The combined group address and group mask must be unique in the system. You cannot write duplicate mappings for the same group or group range.

**Location** PIM-GROUP-RP-MAPPING

## group-mask

**Description** A mask to be applied to the `group-address` value to obtain the group prefix mapped to the specified rendezvous point (RP). For example, a value of 255.0.0.0 indicates a one-octet group prefix. If no mask is specified, the default mask of 255.255.255.255 is applied.

**Usage** Specify an IP address in dotted decimal notation.

**Example** `set group-mask = 255.0.0.0`

**Location** PIM-GROUP-RP-MAPPING

## group-name

**Description** Specifies the name of the view based access control model (VACM) group to which the combination of `security-model` plus `security-name` in the `security-properties` subprofile belongs.

**Usage** Specify a name of up to 23 characters.

**Example** `set group-name = pluto`

**Location** VACM-ACCESS:access-properties  
VACM-SECURITY-GROUP

## group-range-count

**Description** Configures a range of contiguous group addresses in a single filter.

**Usage** The number of group addresses in a range of addresses that begins with the value of the `mcast-ip-address` parameter. Valid values are from 1 to 1024. The default value is 1, which indicates the single address specified as the `mcast-ip-address`.

**Example** `set group-range-count = 20`

**Location** MCAST-SERVICE"" :filter-list [n]

## group-symmetry-mode

**Description** Specifies the symmetry mode of the inverse multiplexing over ATM (IMA) group to which this link belongs.

**Usage** Currently `symmetric-operation` is the only value for this parameter supported.

Symmetric operation entails symmetrical configuration and operation. An IMA link must be configured for each direction of all the physical links to be used, and the IMA unit is only allowed to transmit and receive ATM layer cells over the physical links on which IMA links running in both directions are active.

**Example** `set group-symmetry-mode = symmetric-operation`

**Location** `IMAGROUP`

## gshdsl-psd-type

**Description** Specifies the rate or rates at which a modem outputs a symmetric power spectral density (PSD), based on the G.shdsl standard G.991.2.

**Usage** Valid values are as follows:

- `symmetric` (the default)—The modem outputs a symmetric power spectral density for all rates.
- `asymmetric-776k-psd-annex-a`—The modem outputs an asymmetric power spectral density at 776Kbps only. This parameter is valid only on annex A networks.
- `asymmetric-1544k-psd-annex-a`—The modem outputs an asymmetric power spectral density at 1544Kbps only. This parameter is valid only on annex A networks.
- `asymmetric-2056k-psd-annex-b`—The modem outputs an asymmetric power spectral density at 2056Kbps only. This parameter is valid only on annex B networks.
- `asymmetric-2312k-psd-annex-b`—The modem outputs an asymmetric power spectral density at 2312Kbps only. This parameter is valid only on annex B networks.
- `auto-detect`—Allows customer premise equipment (CPE) to automatically obtain rate setting from central office equipment (COE). Only the CPE can use autodetect.

**Example** `set gshdsl-psd-type = symmetric`

**Location** `HDLSL2:line-config`  
`SHDSL:line-config`

## `gshdsl-standard-network-type`

**Description** Specifies the G.991.2 standard network type for the network that is connected to the single-pair high-rate digital subscriber line (SHDSL) port.

This setting configures a modem to output different characteristics that have been classified for North American and European networks.

**Usage** Valid values are as follows:

- `north-american-annex-a`—North American Annex A network.
- `european-annex-b`—European Annex B network.
- `auto-detect`—Allows customer premise equipment (CPE) to automatically obtain network type setting from central office equipment (COE). Only the CPE can use autodetect.

**Example** `set gshdsl-standard-network-type = north-american-annex-a`

**Dependencies** This parameter applies only if the `interface-type` parameter is set to `g-shdsl`.

**Location** `HDSL2:line-config`  
`SHDSL:line-config`

## H

### h248

**Description** Read-only. Indicates whether H.248 protocol support is enabled or disabled on a Stinger unit.

**Usage** Read-only parameter with one of the following values:

- yes—H.248 protocol support is enabled.
- no—H.248 protocol support is disabled.

**Example** h248 = yes

**Location** BASE

### hardware-level

**Description** Read-only. Indicates a one-character or two-character string representing the hardware revision level of the module.

**Usage** The hardware-level setting is read-only. A value of 0 (zero) means that the revision level is unknown.

**Example** hardware-level = 0

**Location** BASE  
SLOT-INFO

### hardware-revision

**Description** Read-only. Indicates the level of revision for test head hardware in the copper loop test (CLT).

**Usage** The hardware-revision value is read-only.

**Example** hardware-revision = 0

**Location** CLT-RESULT

### hardware-rework-count

**Description** Read-only. Indicates the number of times the module has been reworked.

**Usage** The hardware-rework-count setting is read-only.

**Location** SLOT-INFO

## hardware-ver

**Description** Read-only. Indicates the hardware version of the line interface module (LIM) or of the ADSL modem.

**Usage** The hardware-ver setting is read-only.

**Example** hardware-ver = 1

**Location** AL-DMT-STAT:physical-status  
HDSL2-STAT:physical-status  
SDSL-STAT:physical-status  
SHDSL-STAT:physical-status

## hdlc-rx-crc-error-cnt

**Description** Read-only. Indicates the number of high-level data link control (HDLC) cyclic redundancy check (CRC) errors associated with this channel.

**Usage** Read-only numeric value with a range of 0 to 4294967295.

**Example** hdlc-rx-crc-error-cnt = 28

**Location** SDSL-STAT:physical-statistic

## hds12

**Description** Specifies whether code images for HDSL2 32-port line interface modules (LIMs) are to be stored in flash memory.

**Usage** Valid values are as follows:

- auto—Specifies that the system loads the code image if an HDSL2 32-port LIM is installed. This is the default.
- load—Specifies that the system loads the code image when one is present in the tar file.
- skip—Specifies that the system skips the code image when one is present in the tar file.



**Note** A module is considered present in the system if a slot-type profile exists for that module type. The system creates a slot-type profile when it first detects the presence of a module, and does not delete the profile unless you use the slot -r command to permanently remove a module that is no longer installed in the system, or clear nonvolatile RAM (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.

**Example** set hds12 = auto

**Location** LOAD-SELECT

## hds12-shdsl-threshold-traps-enabled

**Description** Enables or disables HDSL2/SHDSL threshold traps (notifications).

**Usage** Specify one of the following values:

- yes—Enables HDSL2/SHDSL threshold traps. This is the default.
- no—Disables HDSL2/SHDSL threshold traps.

**Example** `set hds12-shdsl-threshold-traps-enabled = no`

**Location** TRAP

## heart-beat-trap-enabled

**Description** Enables/disables the Stinger unit's ability 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.

**Usage** Valid values are as follows:

- yes—Enables heartbeat traps.
- no (the default)—Disables heartbeat traps.

**Example** `set heart-beat-trap-enabled = yes`

**Location** TRAP

## heart-beat-trap-interval

**Description** Time elapsed, in minutes, since the the Stinger unit last generated a trap before it sends a heartbeat trap.

**Usage** Specify a value from 1 through 60. The default value is 5.

**Example** `set heart-beat-trap-interval = 10`

**Location** TRAP

## hec-cell-drop-counter

**Description** Read-only. Indicates the number of cells dropped by header error control (HEC) processing.

**Usage** The `hec-cell-drop-counter` value is read-only.

**Example** `hec-cell-drop-counter = 0`

**Location** OC3-ATM-stat



## hec-correction-enabled

**Description** *Not currently used.* Specifies whether correction of cells received with a single-bit error in the header error control (HEC) is enabled.

**Usage** Valid values are as follows:

- **yes**—Specifies that correction of cells received with a single-bit error in the HEC is enabled.
- **no**—Specifies that correction of cells received with a single-bit error in the HEC is disabled. This is the default.

**Example** `set hec-correction-enabled = no`

**Location** `DS1-ATM:line-config`

## hello-holddown

**Description** Specifies the initial value, in 100ms units, for the Hello hold-down timer used by a Private Network-to-Network Interface (PNNI) node to limit the rate at which it sends Hello packets.

**Usage** Specify a positive nonzero number.

**Example** `set hello-holddown = 10`

**Location** `PNNI-NODE-CONFIG[n]:node-timer`

## hello-hold-time

**Description** Number of seconds a receiver of hello messages must consider the sender reachable before timing out the sender. The value must be greater than that of the `hello-interval` parameter.

**Usage** Specify a number of seconds from 1 to 65535. The default value is 105 seconds.

**Example** `set hello-hold-time = 120`

**Location** `IP-INTERFACE:pim-options`  
`CONNECTION:ip-options:pim-options`

## hello-inactivity-factor

**Description** Specifies the inactivity factor a Private Network-to-Network Interface (PNNI) node uses to determine when a neighbor has stopped operating.

**Usage** Specify a number to designate neighbor inactivity. The default is 10.

**Example** `set hello-inactivity-factor = 5`

**Location** `PNNI-NODE-CONFIG[n]:node-timer`

## hello-interval

**Description** Specifies the interval between Hello packets, as follows:

- For OSPF profiles, specifies the number of seconds between the Hello packets that the Open Shortest Path First (OSPF) router sends on the interface.
- For the node-timer subprofile, specifies the initial value, in seconds, for the Hello timer. In the absence of triggered Hellos, a Private Network-to-Network Interface (PNNI) node sends one Hello packet on each of its ports on this interval.

**Usage** Valid values are as follows:

- For OSPF profiles, specify an integer. The defaults are 10 seconds for connected routes, and 30 seconds for WAN connections and virtual links.
- For the node-timer subprofile, specify a positive nonzero number. The default is 15 seconds.

**Example** `set hello-interval = 10`

**Location** CONNECTION:ip-options:ospf-options

IP-INTERFACE:ospf

OSPF-VIRTUAL-LINK

PNNI-NODE-CONFIG[n]:node-timer

## hello-priority

**Description** Designated router (DR) election priority for the Stinger unit on the interface. The DR election priority is a 32-bit unsigned number contained in a hello message. A router with a numerically larger priority is preferred in electing a new DR.



**Note** Currently, the Stinger unit must not be elected DR on the LAN interface if the LAN supports Internet Group Management Protocol (IGMP) hosts.

**Usage** The valid range for this setting is from 0 to 4,294,967,295, with a default setting of 1.

**Example** `set hello-priority = 0`

**Location** IP-INTERFACE:pim-options

CONNECTION:ip-options:pim-options

## hello-priority-option

**Description** Whether the Stinger unit will participate in Designated router (DR) election on this interface.

**Usage** Valid values are as follows:

- yes (the default)—Enables participation in DR election.
- no—Disables participation in DR election.

**Example** `set hello-priority-option = no`

**Location** IP-INTERFACE:pim-options  
CONNECTION:ip-options:pim-options

## hello-timer

**Description** Specifies the interval, in seconds, between Hello messages sent to the Layer 2 Tunneling Protocol (L2TP) network server (LNS).

**Usage** Specify a number from 0 to 600. The default is 60. The 0 setting specifies that no Hello messages are sent.

**Example** `set hello-timer = 60`

**Location** L2-TUNNEL-GLOBAL:l2tp-config

## high-ber-alarm

**Description** Enables or disables the setting of a relay alarm when the bit-error rate (BER) exceeds the high-ber-alarm-threshold value.

**Usage** Select one of the following values:

- `yes`—Enables setting a relay alarm when the bit-error rate (BER) exceeds high-ber-alarm-threshold.
- `no`—Disables setting a relay alarm when the bit-error rate (BER) exceeds high-ber-alarm-threshold. This is the default.

**Example** `set high-ber-alarm = yes`

**Location** SYSTEM

## high-ber-alarm-threshold

**Description** Specifies the high bit-error rate (BER). When the bit-error rate exceeds the threshold, a relay alarm is set.

**Usage** Select one of the following values:

- `10-**-3`—One error in  $10^3$  bits .
- `10-**-4`—One error in  $10^4$  bits .
- `10-**-5`—One error in  $10^5$  bits .

**Example** `set high-ber-alarm-threshold = 10-**-5`

**Dependencies** For high-ber-alarm-threshold to apply, high-ber-alarm must be set to yes.

**Location** SYSTEM

## high-priority-weight

**Description** Specifies the weight of a queue on the high-priority scheduler. The relative weight determines how much of the scheduler's work cycle this queue can receive relative to other queues on the same scheduler.

**Usage** Specify a value in the range 0 to 15. The total weight per scheduler must be less than or equal to 128. The high-priority weight or low-priority weight must be nonzero if the queue is active.

**Example** `set high-priority-weight = 12`

**Location** SWITCH-CONFIG:atm-parameters:outgoing-queue

## high-tx-output

**Description** Enables or disables high transmit output. This parameter specifies whether the DS3 cable length is more than 255 feet (77.7m).

**Usage** Valid values are as follows:

- For DS3-ATM profiles:
  - `yes`—Specifies that the DS3 cable length is more than 255 feet (77.7m).
  - `no`—Specifies that the DS3 cable length is less than 255 feet. This is the default.

For DS3 cables longer than 255 feet, set this parameter to `yes`.

- For E3-ATM profiles:
  - `yes`—Specifies that the E3 cable length is more than 300 feet (92m).
  - `no`—Specifies that the E3 cable length is less than 300 feet. This is the default.

For E3 cables longer than 300 feet, set this parameter to `yes`.

**Example** `set high-tx-output = yes`

**Location** DS3-ATM:line-config  
E3-ATM:line-config

## history-size

**Description** Enables/disables command logging for a system.

**Usage** Valid values are integers from 0 through 1000. With the default setting of zero (0), command logging is disabled for a Stinger system (the system logs no user commands). The system deletes all existing command logs when a users resets the value of the history-size parameter.

**Example** `set history-size = 100`

**Location** LOG

## hlink-inact

**Description** Specifies the number of seconds the Private Network-to-Network Interface (PNNI) node continues to advertise a horizontal link for which it has not received and processed a logical group node (LGN) horizontal link group.

**Usage** Specify the number of seconds. The default is 120.

**Example** `set hlink-inact = 100`

**Location** `PNNI-NODE-CONFIG[n]:node-timer`

## home-agent-password

**Description** Specifies the password required for Ascend Tunnel Management Protocol (ATMP) tunnel authentication.

Mobile client profiles must supply the password to initiate a tunnel. If the Foreign Agent supplies the proper password when requesting a tunnel, the Home Agent returns a RegisterReply message with a number that identifies the tunnel, and the mobile client's tunnel is established. If the password does not match, the Home Agent rejects the tunnel, and the Foreign Agent logs a message and disconnects the mobile client.

**Usage** Specify a text string of up to 20 characters.

**Example** `set home-agent-password = tunnel-password`

**Location** `ATMP`

## home-network-name

**Description** In an Ascend Tunnel Management Protocol (ATMP) mobile client profile, specifies the name of the gateway profile that defines the connection to the home network when the ATMP Home Agent is operating in gateway mode.

**Usage** If `profile-type` is set to `mobile-client` and `agent-type` is set to `gateway-home-agent`, enter the setting specified for station in the connection profile on the Home Agent. Otherwise, leave the default of null.

**Example** `set home-network-name = myhome`

**Dependencies** This setting applies only when `tunneling-protocol` is set to `atmp-protocol` and `profile-type` is set to `gateway-profile`.

**Location** `CONNECTION:tunnel-options`

## hop-level

**Description** Number of hops (ATM switches) between the Stinger unit and a virtual circuit end point that is permitted to use the queue. This parameter is used to restrict a configured queue for use by virtual circuits originating a certain distance away.

**Usage** Valid values are as follows:

- any-level (the default)—Specifies that virtual circuits originating from a node that is any number of hops away from the Stinger unit are permitted into this queue.
- 0-level—Specifies that virtual circuits originating from a node that is zero hops away are permitted into this queue.
- 1-level—Specifies that virtual circuits originating from a node that is one hop away are permitted into this queue.
- 2-level—Specifies that virtual circuits originating from a node that is two hops away are permitted into this queue.
- 3-level—Specifies that virtual circuits originating from a node that is three hops away are permitted into this queue.

**Example** set hop-level = 1-level

**Location** SWITCH-CONFIG:atm-parameters:outgoing-queue [n]

## host

**Description** Specifies the Domain Name System (DNS) hostname or address of a host on the network, as follows:

- In a connection profile, the host value specifies the first host that the Stinger unit attempts to use for a TCP-clear connection.
- In the ip-global profile, the host value is an array of IP addresses for up to three Simple Network Time Protocol (SNTP) servers. The Stinger unit always queries the first address unless it is inaccessible. In that case, the unit attempts to communicate with the second address, trying the third address only if the other two are inaccessible.
- In the log profile and the auxiliary-syslog[1] and auxiliary-syslog[2] subprofiles of the log profile, the host value specifies the host to which the Stinger unit sends syslog messages for the first, second, and third data stream, respectively.

**Usage** Valid values are as follows:

- For an auxiliary-syslog subprofile, specify the host to which the unit sends syslog messages.
- For a connection profile, specify the name of one or more login hosts to use for TCP-clear connections. You can enter a name of up to 32 characters for each host. The default is null.
- For the ip-global profile, specify up to three IP addresses of SNTP servers, in dotted decimal notation. The default is 0.0.0.0.
- For the log profile, specify the IP address of a UNIX syslog server, in dotted decimal notation. The default is 0.0.0.0.

**Example** Use the following examples to help you set the `host` value:

- The following example sets addresses for the first, second, and third SNTP servers in an `ip-global` profile:
 

```
set host 1 = 1.1.1.1
set host 2 = 1.1.1.2
set host 3 = 1.1.1.3
```
- The following example sets the first login TCP-clear login host in a `connection` profile:
 

```
set tcp-clear-options host = mars
```

**Dependencies** Consider the following:

- In the `log` profile, the `host` value affects all data streams. However, the `host` value in each `auxiliary-syslog` subprofile affects the individual data stream directed to the specified device, and overrides the value in the `log` profile.
- In a `connection` profile, the `host`, `host2`, `host3`, and `host4` values specify the names of up to four login hosts to use for TCP-clear connections. If the TCP connection to the first specified host fails, the system attempts to connect to the next specified host, and so on, up to `host4`. If all connection attempts fail, the session terminates and the Stinger unit returns a TCP connection error to the dial-in client.

**Location** CONNECTION:tcp-clear-options  
 IP-GLOBAL:sntp-info  
 LOG  
 LOG:auxiliary-syslog

host2

host3

host4

**Description** Specifies the name of a login host that the Stinger unit attempts to use for TCP-clear connections.

**Usage** Specify a name of up to 32 characters. The default is null.

**Example** The following examples set addresses for the second, third, and fourth TCP-clear login hosts:

```
set host2 = mercury
set host3 = jupiter
set host4 = saturn
```

**Dependencies** The `host`, `host2`, `host3`, and `host4` values specify the names of up to four login hosts to use for TCP-clear connections. If the TCP connection to the first specified host fails, the system attempts to connect to the next specified host, and so on, up to `host4`. If all connection attempts fail, the session terminates and the Stinger unit returns a TCP connection error to the dial-in client.

**Location** CONNECTION:tcp-clear-options

## host-address

**Description** Specifies the address to which the Stinger unit sends trap (notification) protocol data units (PDUs).

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

**Example** `set host-address = 10.2.3.4/24`

**Dependencies** Consider the following:

- If `host-address` is set to 0.0.0.0 and the Domain Name System (DNS) or Yellow Pages/Network Information System (YP/NIS) is supported, the Stinger unit looks up the host address and sends trap PDUs.
- If `host-address` is set to 0.0.0.0 and `community-name` is null, traps are disabled.

**Location** TRAP

## host-name

**Description** Specifies a hostname or a fully qualified domain name for a hostname-address entry in the local Domain Name System (DNS) table.

**Usage** Specify a hostname or fully qualified domain name. A hostname must be unique within the local DNS table, must start with an alphabetic character, and must have fewer than 256 characters. Trailing periods are ignored in the comparison.

**Example** `set host-name = mercury.abc.com`

**Dependencies** Consider the following:

- If the name does not include a domain name, and you have specified one or more domain-name settings, the system appends the specified domain name when looking up the hostname.
- If `auto-update` is enabled and the corresponding `ip-address` value for a `host-name` setting specifies the default zero address, successful DNS queries will gradually build the local table.

**Location** IP-GLOBAL:dns-local-table:table-config[n]

TRAP

## host-port

**Description** Specifies the port to which traps are sent.

**Usage** Specify a number from 1 to 65535. The default is 162.

**Example** `set host-port = 20`

**Location** TRAP



## hosts-info n

**Description** *Not used.*

**Location** EXT-TSRV

## I

## icmp-reply-directed-bcast

**Description** Enables or disables responding as a host to directed-broadcast Internet Control Message Protocol (ICMP) echo requests.

If an attacker compromises another router on the same Ethernet network as the Stinger unit, ICMP echo requests to the broadcast address might involve the router in denial-of-service attacks. Change this parameter's default setting to prevent the Stinger unit from responding to directed-broadcast ICMP Echo Request packets sent to the IP broadcast address.

**Usage** Specify yes or no. The default is yes.

- yes—Responds to directed-broadcast ICMP echo requests.
- no—Does not respond to directed-broadcast ICMP echo requests.

**Example** `set icmp-reply-directed-bcast = no`

**Location** IP-GLOBAL

## id-auth-prefix

**Description** Specifies the string inserted as a prefix to the telephone number presented to the RADIUS server in caller-ID (CLID) or Dialed Number Information Service (DNIS) authentication requests.

**Usage** Specify a string of up to 16 characters. The default is null.

**Example** `set id-auth-prefix = test`

**Location** EXTERNAL-AUTH:rad-auth-client

## idle-cell-counter

**Description** Read-only. Indicates the total number of idle cells received by the Stinger unit.

**Usage** The idle-cell-counter value is read-only.

**Example** `idle-cell-counter = 0`

**Location** OC3-ATM-STAT

## idle-logout

**Description** Specifies the number of seconds a Telnet session can remain logged in with no keyboard activity.

**Usage** Specify a number of seconds. The default is 0 (zero), which specifies that the station can remain logged in indefinitely.

**Example** `set idle-logout = 60`

**Location** SYSTEM  
USER

## idle-timer

**Description** Specifies a time limit as follows:

- In the `answer-defaults` and `connection` profiles, specifies the number of *seconds* the system waits before clearing a call when a session is inactive (when no packets are being transmitted through the router to the WAN connection).
- In the `atmp` profile, specifies the number of *minutes* that the Home Agent maintains an idle tunnel before disconnecting it.

**Usage** Specify a number from 0 to 65535. A setting a value of 0 (zero) disables the idle timer, so that an idle call or tunnel is maintained indefinitely.

- In the `answer-defaults` and `connection` profiles, the default setting is 120 seconds.
- In the `atmp` profile, the default is 0 (zero) minutes.

**Example** `set idle-timer = 30`

**Location** ANSWER-DEFAULTS:session-info  
ATMP  
CONNECTION:session-options

## idsl-bandwidth

**Description** Specifies the IDSL subscriber bandwidth setting.

**Usage** Valid values are as follows:

- `idsl-128`—IDSL line has 128Kbps available for subscriber data.
- `idsl-144`—IDSL line has 144Kbps available for subscriber data.

**Example** `idsl-bandwidth = idsl-128`

**Location** IDSL:line-interface

## idt-enable

**Description** Specifies whether the internal diagnostic test (IDT) feature is enabled on a line.

**Usage** Valid values are as follows:

- `yes`—Specifies that loopback testing is enabled on the line.
- `no`—Specifies that loopback testing is not enabled on the line. This is the default.

**Example** `set idt-enable = yes`

**Location** `LINE-DIAG`

## idt-error-counter

**Description** Read-only. Indicates the number of error messages received in an internal diagnostic test (IDT).

**Usage** The valid range for this read-only parameter is from 0 to 2147483647.

**Example** `idt-error-counter = 300`

**Location** `LINE-DIAG-STAT`

## idt-num-of-msg

**Description** Specifies the number of messages that the control module sends to the line in an internal diagnostic test (IDT).

**Usage** Enter a number from 0 to 214784647. The default is 1000.

**Example** `set idt-num-of-msg = 2000`

**Location** `LINE-DIAG`

## idt-operation-state

**Description** Specifies whether the internal diagnostic test (IDT) is active on the line.

**Usage** Valid values are as follows:

- `stopped`—Specifies that the test is not active. This is the default.
- `active`—Specifies that the line is undergoing the internal diagnostic test.

**Example** `set idt-operation-state = active`

**Location** `LINE-DIAG-STAT`

### `idt-recv-count`

**Description** Read-only. Indicates the number of messages received by the control module in an internal diagnostic test (IDT).

**Usage** Valid range for this read-only parameter is from 0 to 2147483647.

**Example** `idt-recv-count = 100`

**Location** `LINE-DIAG-STAT`

### `idt-send-count`

**Description** Read-only. Indicates the number of messages sent by the control module in an internal diagnostic test (IDT)

**Usage** Valid range for this read-only parameter is from 0 to 2147483647.

**Example** `idt-send-count = 100`

**Location** `LINE-DIAG-STAT`

### `id-valid`

**Description** Indicates whether the `validation-id` setting in the `remote-shelf-config` profile matches the validation ID specified by the remote shelf's DIP-switch setting.

**Usage** This parameter is read-only. Valid values are as follows:

- `disabled`—No validation was performed.
- `true`—Validation was done, and the software validation ID setting matched the DIP switch setting.
- `false`—Validation was done, and the software validation ID setting did not match the DIP switch setting.

**Location** `REMOTE-SHELF-STAT:validation-status`

### `if-adm-weight-abr`

**Description** Specifies the administrative weight of a Private Network-to-Network Interface (PNNI) for the available bit rate (ABR) service category.

**Usage** Administrative weight is a value used to specify preferential use of a link or node for a specific service category—in this case, for the PNNI ABR category. It is one of the elements of topology-state information exchanged among the nodes, along with a dynamic assessment of available bandwidth, assigned metrics, and other possible attribute values, all of which affect how the most efficient link is chosen at a given time.

Enter a numeric value from 0 to 4294967295. The default value is 5040.

**Example** `set if-adm-weight-abr = 5040`

**Location** `PNNI-IF-CONFIG`

### `if-adm-weight-cbr`

**Description** Specifies the administrative weight of a Private Network-to-Network Interface (PNNI) for the constant bit rate (CBR) service category.

**Usage** Administrative weight is a value used to specify preferential use of a link or node for a specific service category—in this case, for the PNNI CBR category. It is one of the elements of topology state information exchanged among the nodes, along with a dynamic assessment of available bandwidth, assigned metrics, and other possible attribute values, all of which affect how the most efficient link is chosen at a given time.

Enter a numeric value from 0 to 4294967295. The default value is 5040.

**Example** `set if-adm-weight-cbr = 5040`

**Location** `PNNI-IF-CONFIG`

### `if-adm-weight-nrt-vbr`

**Description** Specifies the administrative weight of a Private Network-to-Network Interface (PNNI) for the non-real-time variable bit rate (NRT-VBR) service category.

**Usage** Administrative weight is a value used to specify preferential use of a link or node for a specific service category—in this case, for the PNNI VBR category. It is one of the elements of topology state information exchanged among the nodes, along with a dynamic assessment of available bandwidth, assigned metrics, and other possible attribute values, all of which affect how the most efficient link is chosen at a given time.

Enter a numeric value from 0 to 4294967295. The default value is 5040.

**Example** `set if-adm-weight-nrt-vbr = 5040`

**Location** `PNNI-IF-CONFIG`

### `if-adm-weight-rt-vbr`

**Description** Pertains to the characterization of nodes in the Private Network-to-Network Interface (PNNI). Specifies the administrative weight of this interface for the real-time-variable bit rate (RT-VBR) service category.

**Usage** Administrative weight is a value used to specify preferential use of a link or node for a specific service category. It is one of the elements of topology state information exchanged among the nodes, along with a dynamic assessment of available bandwidth, assigned metrics, and other possible attribute values, all of which affect how the most efficient link is chosen at a given time.

Enter a numeric value from 0 to 4294967295. The default value is 5040.

**Example** `set if-adm-weight-rt-vbr = 5040`

**Location** PNNI-IF-CONFIG

### `if-adm-weight-ubr`

**Description** Specifies the administrative weight of this interface for the unspecified bit rate (UBR) service category.

**Usage** Administrative weight is a value used to specify preferential use of a link or node for a specific service category, in this case for a Private Network-to-Network Interface (PNNI). It is one of the elements of topology state information exchanged among the nodes, along with a dynamic assessment of available bandwidth, assigned metrics, and other possible attribute values, all of which affect how the most efficient link is chosen at a given time.

Enter a numeric value from 0 to 4294967295. The default value is 5040.

**Example** `set if-adm-weight-ubr = 5040`

**Location** PNNI-IF-CONFIG

### `if-aggr-token`

**Description** Specifies the configured aggregation token for the associated Asynchronous Transfer Mode (ATM) interface.

An aggregation token is used to determine which links to a given neighbor node are to be aggregated and used as a single logical link.

**Usage** Enter a numeric value from 0 to 4294967295. The default value is 0.

**Example** `set if-aggr-token = 0`

**Location** PNNI-IF-CONFIG

### `if-auto-spare-info [n]`

**Description** Read-only. Indicates the slot number of port *n* being monitored for automatic port redundancy.

**Usage** A read-only array parameter having one entry for each port on the sparing bus. The individual entry is a numeric value with a range of 0 to 4294967295. The default value is 0, which indicates that the port is not monitored.

**Example** `if-auto-spare-info[2] = 23`

**Location** IF-SPARING-CONFIG

## if-group-index

**Description** Read-only. Indicates the Simple Network Management Protocol (SNMP) interface group index assigned to the line.

**Usage** The if-group-index setting is read-only.

**Example** `if-group-index = 0`

**Location** AL-DMT-STAT:physical-status  
HDSL2-STAT:physical-status  
IDSL-STAT:physical-status  
SDSL-STAT:physical-status  
SHDSL-STAT:physical-status

## if-index

**Description** Specifies the local interface over which the reachable address can be reached.

**Usage** Specify a value. The default, 0 (zero), indicates an unknown interface or reachability through a remote node.

**Example** `set if-index = 0`

**Location** PMNI-ROUTE-ADDR

## if-ip

**Description** Specifies the IP address of one of the IP2000 IP interfaces.

**Usage** Specify an IP address. The default is 0.0.0.0.

**Example** `set if-ip = 10.10.10.10`

**Dependencies** Consider the following:

- If no value is specified in the if-ip field of an enabled circuit-id or remote-id subprofile, the Stinger uses the system address (ip-global:system-ip-addr) if that value has been defined.
- If you set the if-ip value in both the circuit-id and remote-id subprofiles, only one interface IP address is needed.

**Location** IP-GLOBAL:bootp-relay:relay-agent-information:circuit-id  
IP-GLOBAL:bootp-relay:relay-agent-information:remote-id  
BRIDGE-GROUP:dhcp-snooping:circuit-id  
BRIDGE-GROUP:dhcp-snooping:remote-id  
BRIDGE-GROUP:pppoe-snooping:circuit-id  
BRIDGE-GROUP:pppoe-snooping:remote-id

## `if-node-index`

**Description** Specifies the Private Network-to-Network Interface (PNNI) node within the switching system that the interface is directly attached to.

**Usage** Specify a number from 1 to 65535. The value 0 (zero) is not a valid value.

**Example** `set if-node-index = 1`

**Location** PNNI-IF-CONFIG

## `if-number`

**Description** Read-only. Indicates the interface number.

**Usage** The `if-number` value is read-only.

**Example** `if-number = 159`

**Location** ATM-IF-STAT

## `if-port-id`

**Description** Read-only. Indicates the nailed-group number associated with the trunk port.

**Usage** The system assigns each interface a unique default number. This value is read-only.

**Example** `if-port-id = 0`

**Location** PNNI-IF-CONFIG

## `if-rcc-qos-name`

**Description** Specifies the quality-of-service (QoS) contract name for the Private Network-to-Network Interface (PNNI) routing control channel.

**Usage** Specify a contract name with up to 31 alphanumeric characters.

**Example** `set if-rcc-qos-name = pnni-qos-1`

**Location** PNNI-IF-CONFIG



## if-rcc-service-category

**Description** Specifies the service category used for the Private Network-to-Network Interface (PNNI) routing control channel (RCC) on the interface assigned in this profile.

**Usage** Valid values are as follows:

- **cbr**—Constant bit rate. A service class for connections that depend on precise clocking to ensure undistorted delivery of bits.
- **vbr-rt**—Variable bit rate real-time. A service class that handles the packaging of special delay-sensitive applications (such as packet video) that require low cell-delay variation between end points.
- **vbr-nrt**—Variable bit rate non-real-time. A service class that handles packaging for the transfer of long, bursty data streams over a preestablished ATM connection.
- **ubr**—Unspecified bit rate. A service class that handles bursty LAN traffic, as well as data that accepts delays and cell loss. It is a best-effort service that does not specify bit rates or traffic values, and offers no quality of service (QoS) guarantees.

**Example** `set if-rcc-service-category = nrt-vbr`

**Location** PNNI-IF-CONFIG

## if-rcc-traffic-descr-index

**Description** Specifies the traffic descriptor index used for traffic allocation for the Private Network-to-Network Interface (PNNI) routing control channel (VCI = 18) on this interface.

**Usage** The default 2 specifies the default-control service contract used by default for PNNI signaling and routing control.

**Example** `set if-rcc-traffic-descr-index = 2`

**Location** PNNI-IF-CONFIG

## if-remote-address

**Description** Specifies the IP address of the numbered interface at the remote end of a link.

**Usage** Specify the IP address of the numbered interface in dotted decimal notation. The default is 0.0.0.0.

**Example** `set if-remote-address = 10.1.2.3`

**Dependencies** For `if-remote-address` to apply, you must enable IP for the connection profile.

**Location** CONNECTION:ip-options

## if-spare-slot [n]

**Description** Read-only. Indicates the slot number of the redundant (spare) line interface module (LIM) port *n* backing up LIM port *n*.

**Usage** A read-only array parameter having one entry for each port on the sparing bus. If the slot number is 0, then the redundant (spare) LIM port is not being used. This is the default value.

**Example** `if-spare-slot[10] = 5`

**Location** IF-SPARING-CONFIG

## if-spared-slot [n]

**Description** Read-only. Indicates the slot number of the line interface module (LIM) port *n* being replaced by the redundant (spare) LIM port *n*.

**Usage** A read-only array parameter having one entry for each port on the sparing bus. If the slot number is 0, then the port is not being replaced by the redundant (spare) LIM port. This is the default value.

**Example** `if-spared-slot[5] = 10`

**Location** IF-SPARING-CONFIG

## if-sparing-config [n]

**Description** Read-only. Indicates the slot number of the line interface module (LIM) port *n* being replaced by the redundant (spare) LIM port *n*.

**Usage** A read-only array parameter having one entry for each port on the sparing bus. If the slot number is 0, then the port is not being replaced by the redundant (spare) LIM port. This is the default value.

**Example** `if-sparing-config[5] = 10`

**Location** LIM-SPARING-CONFIG

## if-vp-capability

**Description** Enables or disables the ability to establish a virtual private channel (VPC) on the interface.

**Usage** Valid values are as follows:

- `true`—A VPC can be established on this interface.
- `false`—A VPC cannot be established on this interface.

**Example** `set if-vp-capability = false`

**Dependencies** Only physical ATM interfaces can set this parameter to `true`. If it is set to `true` on any other type of interface, the setting is ignored.

**Location** PNNI-IF-CONFIG

## igmp-snooping

**Description** Enables or disables IGMP snooping.

**Usage** Valid values are as follows:

- **yes**—An IP2000 Gigabit Ethernet port must be designated as the MBONE interface for the VLAN by setting the `lan-router-interface-address` parameter.
- **no**—Multicast data streams are forwarded to all ports in the VLAN, even those who have not registered for the multicast. This is the default value.

**Example** `set igmp-snooping = yes`

**Location** BRIDGE-GROUP

## ignore-cell-delay-variation-tolerance

**Description** Enables or disables the system's use of cell delay variation tolerance (CDVT).

**Usage** Valid values are as follows:

- **yes**—The `cell-delay-variation-tolerance` parameter is ignored. This internal parameter is used to tolerate bursty customer premises equipment (CPE) that has inadequate or no traffic shaping capability. This is the default.
- **no**—The `cell-delay-variation-tolerance` parameter is not ignored.

**Example** `set ignore-cell-delay-variation-tolerance = no`

**Dependencies** When this parameter is set to `no`, the `ignore-max-burst-size` parameter is applied.

This parameter does not apply when PCR policing is disabled. PCR policing is disabled when `peak-rate-kbits-per-sec` and `cell-delay-variation-tolerance` values are set to zero.

**Location** ATM-QOS

## ignore-def-route

**Description** Enables or disables exclusion of advertised default routes from updates to the routing table.

Enabling this feature protects the system's local default route from being modified by RIP updates.

**Usage** Valid values are as follows:

- **yes**—The system does not add advertised default routes to the local routing table. This setting (which is recommended) prevents updates from modifying the default route in the routing table. This is the default.
- **no**—The system includes advertised default routes in routing table updates.

**Example** `set ignore-def-route = no`

**Location** IP-GLOBAL

## ignore-icmp-redirects

**Description** Enables or disables processing of Internet Control Message Protocol (ICMP) Redirect packets.

ICMP Redirect packets can be counterfeited and used to change the way a device routes packets. For security purposes, many sites choose to ignore ICMP redirects.

**Usage** Valid values are as follows:

- **yes**—The system ignores ICMP Redirect packets.
- **no**—The system processes ICMP Redirect packets normally. This is the default.

**Example** `set ignore-icmp-redirects = yes`

**Location** IP-GLOBAL

## ignore-lineup

**Description** This parameter is used differently in the system profile and in a line profile. A line profile is a profile for a particular line type (al-dtm, ds1-atm, e3-atm, and so on).

- In a line profile, `ignore-lineup` specifies whether the line status of a slot determines the Stinger call-control mechanism on a specified port.
- In the system profile, `ignore-lineup` specifies whether the Stinger unit ignores line status when determining whether calls are established.

**Usage** Valid values are as follows:

- In a line profile, specify one of the following values for this parameter:
  - **system-defined**—Sets the Stinger unit to inherit the `ignore-lineup` value from the system profile. This is the default.
  - **no**—Sets the Stinger call-control mechanism to ignore the system-wide `ignore-lineup` setting and allows calls to be established when the line state is UP and disallow calls on the port when the line state is DOWN.
  - **yes**—Sets the Stinger call-control mechanism to ignore both the line state and the system-wide setting and allows calls to be established on the specified port as long as the specified slot is operational and the specified port is enabled.
- In the system profile, specify one of the following values for this parameter:
  - **no**—The Stinger call-control mechanism allows calls to be established when the line state is UP and disallow calls when the line state is DOWN. This is the default.
  - **yes**—The Stinger call-control mechanism ignores the line state and allows calls to be established on a port as long as the specified slot is operational and the specified port is enabled.

**Example** `set ignore-lineup = yes`

**Location** AL-DMT  
DS1-ATM  
DS3-ATM  
E3-ATM  
HDSL2  
IDSL:line-interface  
IMAGROUP  
OC3-ATM  
SHDSL  
SDSL  
SYSTEM

## `ignore-max-burst-size`

**Description** Enables or disables the system's use of the `max-burst-size` parameter setting.

**Usage** Valid values are as follows:

- `yes`—Specifies the `max-burst-size` parameter is ignored. Instead an internal parameter is used to tolerate bursty customer premises equipment (CPE) that does not have or has inadequate traffic shaping capability. This is the default.
- `no`—Specifies that the `max-burst-size` parameter is applied.

**Example** `set ignore-max-burst-size = no`

**Dependencies** This parameter does not apply when SCR policing is disabled. SCR policing is disabled when `sustainable-rate-kbits-per-sec` and `max-burst-size` values are set to zero.

**Location** ATM-QOS

## `ilmi-admin-status`

**Description** Enables or disables Integrated Local Management Interface (ILMI) connectivity procedures. *ILMI is not supported with the current software version.*

**Usage** This parameter must be set to `yes` to enable ILMI connectivity procedures. Specify one of the following values:

- `yes`—Enables ILMI connectivity.
- `no` (the default)—Disables ILMI connectivity.

**Example** `set ilmi-admin-status = yes`

**Dependencies** ILMI connectivity is enabled only when both `ilmi-admin-status` and `ilmi-connectivity` are set to `yes`. ILMI connectivity is disabled if `ilmi-admin-status` or `ilmi-connectivity` is set to `no`.

**Location** ATM-IF-CONFIG:extension-config

## ilmi-connectivity

**Description** Enables or disables Integrated Local Management Interface (ILMI) connectivity procedures. *ILMI is not supported with the current software version.*

**Usage** Specify one of the following values:

- yes—Enables ILMI connectivity.
- no (the default)—Disables ILMI connectivity.

**Example** set ilmi-connectivity = yes

**Dependencies** ILMI connectivity is enabled only when both ilmi-admin-status and ilmi-connectivity are set to yes. ILMI connectivity is disabled if ilmi-admin-status or ilmi-connectivity is set to no.

**Location** ATM-IF-CONFIG:extension-config

## ilmi-link-state

**Description** Read-only. Specifies the Integrated Local Management Interface (ILMI) link state of the port. *ILMI is not supported with the current software version.*

**Usage** Read-only parameter with one of the following values:

- not-configured—The component is not configured. This is the default.
- up—The component is in UP state.
- down—The component is in DOWN state.

**Example** ilmi-link-state = up

**Location** ATM-IF-STAT

## ilmi-vci

**Description** *Integrated Local Management Interface (ILMI) is not supported with the current software version.* Specifies the virtual channel identifier (VCI) value for the virtual channel connection (VCC) supporting the ILMI at this ATM interface

**Dependencies** If this value and the value of the ilmi-vpi parameter are both equal to zero then the ILMI is not supported at this ATM interface.

**Example** set ilmi-vci = 0

**Location** ATM-IF-CONFIG:base-config

## ilmi-vpi

**Description** *Integrated Local Management Interface (ILMI) is not supported with the current software version.* Specifies the virtual channel identifier (VCI) value for the virtual channel connection (VCC) supporting the ILMI at this ATM interface.

**Dependencies** If this value and the value of the ilmi-vci parameter are both equal to 0 (zero) then the ILMI is not supported at this ATM interface.

**Example** `set ilmi-vpi = 0`

**Location** `ATM-IF-CONFIG:base-config`

## ima

**Description** Specifies whether code images for T1 and E1 modules are to be stored in flash memory.

**Usage** Valid values are as follows:

- `auto`—Specifies that the system loads the code image if a T1 or E1 module is installed. This is the default.
- `load`—Specifies that the system loads the code image when one is present in the tar file.
- `skip`—Specifies that the system skips the code image when one is present in the tar file.



**Note** A module is considered present in the system if a `slot-type` profile exists for that module type. The system creates a `slot-type` profile when it first detects the presence of a module, and does not delete the profile unless you use the `slot -r` command to permanently remove a module that is no longer installed in the system, or clear nonvolatile RAM (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.

**Example** `set ima = auto`

**Location** `LOAD-SELECT`

## ima-enabled

**Description** Read-only. Indicates the status of the inverse multiplexing over ATM (IMA) feature.

**Usage** Read-only parameter with one of the following values.

- `yes`—IMA feature is enabled.
- `no`—IMA feature is not enabled.

**Example** `ima-enabled = yes`

**Location** `BASE`

## ima-id

**Description** Specifies the inverse multiplexing over ATM (IMA) identifier of the IMA group.

**Usage** Specify a number from 0 (zero) to 255.

**Example** `set ima-id = 7`

**Location** `IMAGROUP`

## ima-violations-counter

**Description** Read-only. Indicates the number of inverse multiplexing over ATM (IMA) Control Protocol (ICP) violations.

ICP violations are errored, invalid, or missing ICP cells in a 15-minute interval. This value does indicate severely errored seconds-IMA (SES-IMA) or unavailable-seconds-IMA (UAS-IMA) conditions.

**Usage** The valid range is from 0 (zero) to 2147483647.

**Example** ima-violations-counter = 0

**Location** DS1-ATM-STAT:ima-link-statistic

## impulse-noise-read-high-threshold

**Description** Read-only. Indicates the number of impulse events with levels exceeding the threshold value plus 2delta in a copper loop test (CLT).

**Usage** The value is read-only.

**Example** impulse-noise-read-high-threshold = 0

**Location** CLT-RESULT

## impulse-noise-read-low-threshold

**Description** Read-only. Indicates the number of impulse noise events with levels between the threshold and the threshold plus delta in a copper loop test (CLT).

**Usage** The value is read-only.

**Example** impulse-noise-read-low-threshold = 0

**Location** CLT-RESULT

## impulse-noise-read-mid-threshold

**Description** Read-only. Indicates the number of impulse events with levels between threshold plus delta and threshold plus 2delta in a copper loop test (CLT).

**Usage** The value is read-only.

**Example** impulse-noise-read-mid-threshold = 0

**Location** CLT-RESULT

## impulse-noise-start-dead-time

**Description** Specifies the measurement delay, in tenths (0.1) of a millisecond, after the Stinger unit detects the initial impulse in a copper loop test (CLT).

**Usage** Specify a number from 10 to 2550.



**Example** `set impulse-noise-start-dead-time = 11`

**Location** CLT-COMMAND

## `impulse-noise-start-delta`

**Description** Specifies the amount above threshold, in decibels below 1 milliwatt (dBm), for noise spike detection in a copper loop test (CLT).

**Usage** Specify a number from 2 to 6.

**Example** `set impulse-noise-start-delta = 4`

**Location** CLT-COMMAND

## `impulse-noise-start-max-count`

**Description** Specifies the maximum number of impulse events to be counted during a single measurement in a copper loop test (CLT).

**Usage** Specify a number from 1 to 9999.

**Example** `set impulse-noise-start-max-count = 200`

**Location** CLT-COMMAND

## `impulse-noise-start-thresh`

**Description** Specifies the threshold value, in decibels below 1 milliwatt (dBm), of the smallest noise spike detected in a copper loop test (CLT).

**Usage** Specify a number from 50 to 100.

**Example** `set impulse-noise-start-thresh = 60`

**Location** CLT-COMMAND

## `impulse-noise-start-timer`

**Description** Specifies the duration, in minutes, of impulse noise measurement in a copper loop test (CLT).

**Usage** Specify a number from 1 to 9999.

**Example** `set impulse-noise-start-timer = 30`

**Location** CLT-COMMAND

## `inactivity-time`

**Description** Specifies how long the unit waits before disconnecting an inactive modem connection.

**Usage** Specify a number of seconds from 0 through 255. The default is 0 (zero), which specifies that an inactive modem connection is not disconnected after any period of inactivity.

**Example** `set inactivity-time = 60`

**Location** MODEM

## `inauguration-time`

**Description** Read-only. Indicates the time at which the controller in this context started waiting for the other controller to load the operational software.

**Usage** Read-only parameter with a numeric range of 0 to 4294967295.

**Example** `inauguration-time = 12324`

**Location** REDUNDANCY-STATS:context-stats

## `incoming-cells`

**Description** Read-only. Indicates the number of cells coming in on the interface.

**Usage** This read-only statistic helps you verify the operation of the physical interface.

**Example** `incoming-cells = 92`

**Location** AL-DMT-STAT:physical-statistic

## `incoming-priority`

**Description** Specifies the relative priority of Asynchronous Transfer Mode (ATM) cells incoming from this line interface module (LIM) or control module slot.

**Usage** Valid values are as follows:

- `high-priority`—ATM cells incoming from this LIM or control module slot have a higher priority than others.
- `low-priority`—ATM cells incoming from this LIM or control module slot have a lower priority than others. This is the default.

**Example** `set incoming-priority = high-priority`

**Location** HIGH-SPEED-SLOT-STATIC-CONFIG:atm-parameters

## increment-channel-count

**Description** Specifies the number of channels the Stinger unit adds for a manual or automatic bandwidth change during a call.

**Usage** Specify an number from 1 to 32. The default is 1.

**Example** set increment-channel-count = 3

**Location** ANSWER-DEFAULTS:mpp-answer  
CONNECTION:mpp-options

## in-defect-int-time

**Description** *Not currently used.* Specifies the maximum amount of time, in milliseconds, allowed for the system to learn the receiving link ID (RX LID) in intelligent call processing (ICP) cells.

If the defect is persistent for this time, the link enters the FAILED state.

**Usage** The valid range is from 0 (zero) to 2147483647.

**Example** set in-defect-int-time = 2500

**Location** DS1-ATM:line-config:ima-option-config:rxlink-config

## index

**Description** Indicates an internal index, or distinguishes between multiple listings.

**Usage** Valid values are as follows:

- In the index subprofile of the error profile, the value of the index parameter indicates the internal index of the entry. The index setting is read-only.
- In the index subprofile of the atm-spvc-addr-config profile, you specify the value of the index parameter to distinguish between multiple listings of connectivity to a given address prefix from the local node.
- In the index subprofile of the call-route profile, you specify the index of this call routing profile entry. The index contains the physical address of the device to which a call can be routed and an entry number allowing multiple entries for a device.
- The index parameter of the cmd-log profile is the index number of the command log. This parameter is read-only.

**Example** index = mithra0

**Location** ATM-SPVC-ADDR-CONFIG  
CALL-ROUTE  
cmd-log  
ERROR

## *index-name*

**Description** Specifies the name of the `pnmi-summary-addr` profile corresponding to the values of the `addr-index` subprofile.

**Usage** Specify an index name up to 50 alphanumeric characters in length.

**Example** `set index name = summary_addr_one`

**Location** `PNMI-SUMMARY-ADDR`

## *inet-profile-type*

**Description** Read-only. Indicates whether the dedicated (nailed-up) profile associated with the hostname in the `admin-state-perm-if` profile is a local profile or a profile from the RADIUS server.

**Usage** The `inet-profile-type` setting is read-only. The number 0 (zero) indicates a local profile. The number 1 (one) indicates a RADIUS profile.

**Example** `inet-profile-type = 1`

**Location** `ADMIN-STATE-PERM-IF`

## *info*

**Description** *Not used.* Specifies a reference to management information base (MIB) definitions specific to the routing protocol set in the `proto` parameter.

**Usage** This parameter is currently set to the null string.

**Example** `set info = ""`

**Location** `PNMI-ROUTE-ADDR`

## *information*

**Description** Command-line interface command entered by the user.

**Usage** This parameter is read-only.

**Example** `information = "dir cmd-log"`

**Location** `cmd-log`

## *inform-retry-count*

**Description** Read-only. Indicates the number of retries attempted when acknowledgement is not received for an Inform protocol data unit (PDU).

**Usage** This parameter is read-only. The valid range is from 0 to 2147483637. The default is 4.

**Example** `inform-retry-count = 10`

**Location** `TRAP`

## inform-time-out

**Description** *Not used.* Read-only. Indicates the timeout interval in units of 0.01 seconds after which the Inform protocol data unit (PDU) is retransmitted on receiving no acknowledgement.

**Usage** This parameter is read-only. The valid range is from 0 to 2147483637. The default is 1500.

**Example** `inform-time-out = 1000`

**Location** `TRAP`

## init-banner n

**Description** *Not used.*

**Location** `EXT-TSRV`

## initial-adsl-ver

**Description** Read-only. Indicates the number of changes made to the Alcatel Proprietary Exchange phase in this version of the software.

**Usage** The `initial-adsl-ver` value is read-only. The current value is 1.



**Note** This parameter is valid only for the ADSL 12-port LIM, which is based on the Alcatel chipset.

**Example** `initial-adsl-ver = 1`

**Dependencies** Both ends of the connection must agree on the value of `initial-adsl-ver` parameter for the chip sets to take advantage of the advanced functionality supported by Alcatel equipment.

**Location** `AL-DMT-STAT:physical-status`

## initialization-time

**Description** Read-only. Indicates the time at which the controller in this context sets its function.

**Usage** Read-only parameter with a numeric range of 0 to 4294967295.

**Location** `REDUNDANCY-STATS:context-stats`

## init-time

**Description** Specifies the number of seconds the Private Network-to-Network Interface (PNNI) node delays advertising its choice of the preferred peer group leader (PGL), after having initialized operation and reached the full state with a least one neighbor in the peer group.



**Note** This parameter is not currently supported in the `node-svcc-rcc` subprofile.

**Usage** Specify the number of seconds.

**Example** `set init-time = 15`

**Location** PNNI-NODE-CONFIG [n] :node-pgl  
PNNI-NODE-CONFIG [n] :node-svcc-rcc

## installation-complete

**Description** Read-only. Indicates whether the first-time installation menu has been run and NVRAM first initialized.

**Usage** Read-only parameter with the following possible values:

- `yes`—NVRAM has not been first initialized.
- `no`—NVRAM has been first initialized.

**Example** `installation-complete = no`

**Location** SYSTEM

## interface-address

**Description** Specifies the physical address of the Ethernet interface in the Stinger unit, or, if the item number is not zero, the IP virtual interface address.

**Usage** In most cases, the `interface-address` value is obtained from the system. However, you can modify it in an `ip-interface` profile to create a new virtual interface profile from an existing profile.

**Example** `set interface-address logical-item = 1`

**Location** ETHERNET  
ETHERNET-INFO  
IP-INTERFACE  
VLAN-ETHERNET

## interface-group

**Description** Interface group number.

**Usage** 0 through 255. The default value is 0.

**Example** `set interface-group = 20`

**Dependencies** If the group number assigned to the incoming interface does not match the `interface-group` of the rule, the comparison fails.

**Location** `PACKET-FLOWS/"":flow[n]:packet-classifier`

## interface-sparing-enabled

**Description** Specifies whether the interface (port) redundancy trap (notification) is to be sent to the identified host.

**Usage** Valid values are as follows:

- `yes`—Specifies that the interface (port) redundancy trap is sent to the identified host. This is the default.
- `no`—Specifies that the interface (port) redundancy trap is not sent to the identified host.

**Example** `set interface-sparing-enabled = yes`

**Dependencies** Only when this parameters is set to `no` can the SNMP agent in a Stinger unit report traps to an SNMP manager.

**Location** `TRAP`

## interface-type

**Description** Specifies or indicates the mode of operation for an single-pair high-rate digital subscriber line (SHDSL)/high-rate digital subscriber line 2 (HDSL2) 32-port line interface module (LIM).

**Usage** Following are valid values:

- For the `slot-static-config` profile, specify one of the following values:
  - `g-shdsl` (default)—The LIM operates in SHDSL mode and supports symmetric data rates from 72Kbps to 2312Kbps.
  - `hdsl2`—The LIM operates in HDSL2 mode and supports symmetric data transfer at 1.544Mbps over a single twisted pair.
  - `default`—The default mode of operation of the LIM that is inserted into the slot. For the SHDSL/HDSL2 32-port LIM, the default is `g-shdsl`.
- For the `hdsl2-stat` or `shdsl-stat` profile, this parameter has the following read-only values:
  - `g-shdsl`—The LIM is operating in SHDSL mode.
  - `hdsl2`—The LIM is operating in HDSL2 mode.
  - `default`—The LIM is not a HDSL2/SHDSL LIM.
- For the `transceiver-info` profile, this parameter has the following read-only values which indicate the card type in the applicable slot:
  - `interface-oc12`—Indicates an OC12 card.
  - `interface-none`—Indicates no card is detected.
  - `interface-oc3`—Indicates an OC3 card.

**Example** `set interface-type = hdsl2`

**Dependencies** If this parameter is set to `hds12`, the `rate-mode`, `min-rate`, and `max-rate` parameters do not apply in the `line-config` subprofile of the `hds12` profile.

**Location** `HDSL2-STAT:physical-status`  
`SHDSL-STAT:physical-status`  
`SLOT-STATIC-CONFIG`  
`TRUNK-DAUGHTER-DEV:transceiver-info`

## `internal-fan-unit-failed`

**Description** An alarm was received from the remote shelf fan to indicate a failure of the internal fan unit.

**Usage** This parameter is read-only. Valid values are as follows:

- `yes`—An alarm was received.
- `no` (the default)—No alarms were received.

**Location** `REMOTE-SHELF-STAT`

## `interval-auto-correction`

**Description** Specifies the interval, in milliseconds, during which a line interface module (LIM) attempts autocorrection.

Some LIMs are capable of performing detection before correction. These LIMs attempt to detect the problem and then correct it.

**Usage** Specify a value from 0 to 2147483647. The default is 12000ms.

**Example** `set interval-auto-correction = 500000`

**Location** `SYSTEM-INTEGRITY:integrity-config`

## `inter-vrouter`

**Description** Specifies the name of a virtual router (VRouter) to use as the route's next hop. All packets to the static route's destination network are sent to the specified virtual router for a routing decision.

**Usage** Specify the name of a defined virtual router. The default is null, which represents the global virtual router (the main IP router).

**Example** `set inter-vrouter = vrouter-1`

**Dependencies** The `gateway-address` parameter must be set to the zero address for this parameter to apply.

**Location** `IP-ROUTE`



## intra-community

**Description** *Not used.* Specifies the highest level of the Private Network-to-Network Interface (PNNI) hierarchy that lies within the intracommunity scope.

**Usage** Specify a number from 0 to 104. The default value is 48.

**Example** `set intra-community = 50`

**Location** PNNI-NODE-CONFIG [n] :node-scope-mapping

## intra-organization

**Description** *Not used.* Specifies the highest level of the Private Network-to-Network Interface (PNNI) hierarchy that lies within the intraorganization scope.

**Usage** Specify a number from 0 to 104. The default value is 64.

**Example** `set intra-organization = 75`

**Location** PNNI-NODE-CONFIG [n] :node-scope-mapping

## intra-regional

**Description** *Not used.* Specifies the highest level of the Private Network-to-Network Interface (PNNI) hierarchy that lies within the interregional scope.

**Usage** Specify a number from 0 to 104. The default value is 32.

**Example** `set intra-regional = 35`

**Location** PNNI-NODE-CONFIG [n] :node-scope-mapping

## intra-site

**Description** *Not used.* Specifies the highest level of the Private Network-to-Network Interface (PNNI) hierarchy that lies within the intrasite scope.

**Usage** Specify a number from 0 to 104. The default value is 80.

**Example** `set intra-site = 86`

**Location** PNNI-NODE-CONFIG [n] :node-scope-mapping

## invalid-intervals

**Description** Read-only. Indicates the number of 15-minute intervals for which no valid data is available.

**Usage** The valid range for this read-only parameter is from 0 (zero) to 96.

**Example** invalid-intervals = 0

**Location** DS1-ATM-STAT:ima-link-status  
IMA-GROUP-STAT

## ip-address

**Description** Specifies or indicates an IP address, as follows:

- In an ip-interface profile, the value is the IP address of a virtual IP or Ethernet interface.
- In the Domain Name System (DNS) local table definition in the ip-global profile, the value is a valid IP address for the host-name setting, or the zero address.  
  
If auto-update is enabled and ip-address specifies the default zero address, successful DNS queries will gradually build the local table.
- In an error profile, the ip-address parameter is read-only and indicates the address or subnet from which an operator reset was requested.

**Usage** Specify an IP address in dotted decimal notation. The default is the null address (0.0.0.0/0).

In an error profile, the default is 0.0.0.0.

**Example** set ip-address = 1.1.1.1/32

**Location** ERROR  
IP-GLOBAL:dns-local-table:table-config[n]  
IP-INTERFACE

## ip-direct

**Description** Specifies the IP address of a host to which the system directs all IP packets received across the link, without consulting the IP routing table.

**Usage** Specify an IP address in dotted decimal notation. The default is the null address (0.0.0.0/0).

**Example** set ip-direct = 1.1.1.10/28

**Location** CONNECTION:ip-options

## ipport-cache-enable

**Description** *Not supported.* Enables or disables module-to-module IP packet forwarding based on the packet destination IP address and port. This setting is not used by the router module, which supports its own router subsystem.

**Location** IP-GLOBAL

## ip-protocol

**Description** Protocol number.

**Usage** Zero matches all protocols. A nonzero number is compared to the Protocol field in each packet. For a list of assigned protocol numbers, see RFC 1700, *Assigned Numbers*. The default value is 0.

**Example** `set ip-protocol = 4`

**Dependencies** If the protocol field of the packet does not match the ip-protocol of the rule, the rule comparison fails.

**Location** `PACKET-FLOWS/"":flow[n]:packet-classifier`

## iproute-cache-enable

**Description** *Not supported.* Enables or disables the route cache. This setting is not used by the router module, which supports its own router subsystem.

**Location** `IP-GLOBAL`

## iproute-cache-size

**Description** *Not supported.* Specifies the size of the internal route cache. This setting is not used by the router module, which supports its own router subsystem.

**Location** `IP-GLOBAL`

## ip-routing-enabled

**Description** Enables or disables IP routing for the interface.

IP routing is typically disabled in Asynchronous Transfer Mode (ATM) circuit configurations, and enabled in terminating connections or those that are switched internally for routing to the router module.

**Usage** Valid values are as follows:

- `yes` (the default)—Enables IP routing on the WAN interface.
- `no`—Disables IP routing on the interface.

**Example** `set ip-routing-enabled = no`

**Location** `CONNECTION:ip-options`

## ip-tos

**Description** Number to be compared to the second octet (IP TOS bits) in IP packet headers.

**Usage** Valid values are from 0 through 255. The default value is 0.

**Example** `set ip-tos = 4`

**Dependencies** If the 8 TOS bits in the header of the incoming packet do not match the `ip-tos` of the rule, the comparison fails.

**Location** `PACKET-FLOWS/"":flow[n] :packet-classifier`

## *is-post*

**Description** Read-only. Indicates whether the error specified in the `error` profile occurred during a power-on self test (POST).

**Usage** The `is-post` setting is read-only. Valid values are as follows:

- `yes`—Indicates that the error occurred during a POST.
- `no`—Indicates that the error did not occur during a POST.

**Example** `is-post = no`

**Location** `ERROR`

## *item-number*

**Description** Specifies an item on a line interface module (LIM) or trunk module. Items are numbered starting with 1 for the topmost or leftmost item on the module. For example:

- In a Stinger FS, Stinger FS+, Stinger LS, or Stinger RT, line 48 on a LIM in slot 2 has the following address: `{ 1 2 48 }`.
- In a Stinger MRT, line 4 on a T1 trunk module has the following address: `{ 1 18 4 }`

**Usage** Specify a number from 0 to 65535. The default is 0 (zero), which denotes the entire slot.

**Example** `set item-number = 24`

**Location** `DEVICE-ADDRESS`  
`PHYSICAL-ADDRESS`

---

## j

### join-prune-interval

**Description** Number of seconds between sending Protocol Independent Multicast (PIM) join/prune messages to PIM neighbors on this interface. A join/prune message consists of a list of groups and a list of joined and pruned sources for each group. The value must be less than that of the `join-prune-holdtime` parameter.



**Note** Stinger units do not currently support the (S,G) state, so it always sends (\*,G) join/prune messages.

**Usage** The valid range is from 1 to 65535 with a default value of 60 seconds.

**Example** `set join-prune-interval = 30`

**Location** IP-INTERFACE:pim-options  
CONNECTION:ip-options:pim-options

### join-prune-holdtime

**Description** Number of seconds a receiver of join/prune messages must consider the list valid before timing out the information. The value must be greater than that of the `join-prune-interval` parameter.

**Usage** The valid range is from 1 to 65535 with a default value of 210 seconds.

**Example** `set join-prune-holdtime = 180`

**Location** IP-INTERFACE:pim-options  
CONNECTION:ip-options:pim-options

## K

### key-id

**Description** Specifies a value used to encrypt the secret key when `authen-type` is set to `md5`.

**Usage** Specify a number from 0 through 255. The default is 0 (zero).

**Example** `set key-id = 10`

**Dependencies** For `key-id` to apply, you must set `authen-type` to `md5`.

**Location** CONNECTION:ip-options:ospf-options  
IP-INTERFACE:ospf  
OSPF-VIRTUAL-LINK

## L

### l2tp-auth-enabled

**Description** Enables or disables Layer 2 Tunneling Protocol (L2TP) tunnel authentication.

**Usage** Values are as follows:

- `yes`—Authenticates the L2TP network server (LNS) before passing calls to the system.
- `no` (the default)—Does not authenticate the LNS.

**Example** `set l2tp-auth-enabled = yes`

**Dependencies** If you are using RADIUS with L2TP, the RADIUS server must be able to encrypt the `tunnel-password` attribute.

**Location** `L2-TUNNEL-GLOBAL`

### l2tp-enabled

**Description** Read-only. Indicates the status of the Layer 2 Tunneling Protocol (L2TP) feature.

**Usage** Read-only parameter with one of the following values:

- `no`—L2TP feature is not enabled.
- `yes`—L2TP feature is enabled.

**Example** `l2tp-enabled = yes`

**Location** `BASE`

### l2tp-mode

**Description** Enables or disables Layer 2 Tunneling Protocol (L2TP) operations.

**Usage** Values are as follows:

- `lac`—Enables L2TP access concentrator (LAC) operations.
- `lns`—*Not supported.*
- `both`—*Not supported.*
- `disabled` (the default)—Disables L2TP functionality.

**Example** `set l2tp-mode = lac`

**Location** `L2-TUNNEL-GLOBAL`

## l2tp-rx-window

**Description** Specifies the Layer 2 Tunneling Protocol (L2TP) receive window size to advertise for data channels.

**Usage** The valid range is from 0 to 63. The 0 (zero) default specifies that the L2TP access concentrator (LAC) requests no flow control for inbound L2TP payloads. A nonzero value enables behavior that predates RFC 2661.



**Note** Not all L2TP implementations support a nonzero value. Be careful to ensure that the L2TP network server (LNS) supports a nonzero value for this parameter before changing the default.

**Example** `set l2tp-rx-window = 63`

**Location** L2-TUNNEL-GLOBAL

## l2tp-system-name

**Description** Specifies a name that can be sent to the Layer 2 Tunneling Protocol (L2TP) network server (LNS) during tunnel authentication.

**Usage** Enter a string of up to 31 characters. The default is null.

**Example** `set l2tp-system-name = lac-1`

**Dependencies** If you specify a value of more than 31 alphanumeric characters, the hostname passed to the L2TP end point is truncated and the plus (+) sign is appended to it.

**Location** L2-TUNNEL-GLOBAL

## lac-incoming-call-timer

**Description** Specifies the number of seconds the system waits for an incoming session request to complete.

**Usage** Specify a number from 1 to 600. The default is 60.

**Example** `set lac-incoming-call-timer = 120`

**Location** L2-TUNNEL-GLOBAL:l2tp-config

## lan-delay

**Description** Number of milliseconds of expected propagation delay over the Ethernet interface.

**Usage** The valid range is from 1 to 65535 with a default value of 5000 milliseconds.

**Example** `set lan-delay = 1000`

**Location** IP-INTERFACE:pim-options  
CONNECTION:ip-options:pim-options

## lan-delay-option

**Description** Whether the Stinger unit expects propagation delay over an Ethernet interface (yes or no, with a default value of yes).

**Usage** Valid values are as follows:

- yes (the default)—The Stinger unit expects propagation delay.
- no—The Stinger unit does not expect propagation delay.

**Example** `set lan-delay-option = no`

**Location** IP-INTERFACE:pim-options  
CONNECTION:ip-options:pim-options

## lasr

**Description** Specifies whether link addition and slow recovery (LASR) procedures are enabled or disabled.

**Usage** Valid values are as follows:

- yes—Specifies that LASR is enabled. This is the default.
- no—Specifies that LASR is disabled.

**Example** `set lasr = no`

**Location** IMAGROUP

## last-32

**Description** Read-only. Indicates a 32-bit mask to track the last 32 times this device is tried.

**Usage** The last-32 value is read-only. A 0 (zero) in the bit position indicates failure, while a 1 (one) indicates success. Numeric values range from 0 through 4294967295. The value 0 is the default.

**Example** `last-32 = 1028`

**Location** DEVICE-STATE

## last-change-time

**Description** Read-only. The number of seconds or milliseconds that have lapsed since the inverse multiplexing over ATM (IMA) group last changed state.

**Usage** The last-change-time value is read-only. Valid values range from zero to 2147483647.

**Example** `last-change-time = 1320`

**Location** IMA-GROUP-STAT:ima-rt



## last-code-sync

**Description** Read-only. Indicates the time at which the controller in this context last synchronized its code repository with its partner.

**Usage** Read-only parameter with a numeric range of 0 to 4294967295.

**Example** last-code-sync = 123

**Location** REDUNDANCY-STATS:context-stats

## last-login-date

**Description** Date when this user profile was last used to log into the system.

**Usage** This parameter is read-only.

**Example** last-login-date = { Wednesday November 2003 12 }

**Location** USER

## last-log-recv

**Description** Read-only. Indicates the time at which the controller in this context last received a fatal log entry from its partner.

**Usage** Read-only parameter with a numeric range of 0 to 4294967295.

**Example** last-log-recv = 123

**Location** REDUNDANCY-STATS:context-stats

## last-member-query-count

**Description** Specifies the number of group-specific queries sent before the multicast router assumes there are no local members.

**Usage** Specify an integer.

**Example** set last-member-query-count = 10

**Location** CONNECTION:ip-options:igmp-options

## last-member-query-interval

**Description** Specifies the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to Leave Group messages.

**Usage** Specify a number from 0 through 1024. You can reduce this value from its default of 1 second to reduce the time it takes to detect that the last member of a group has left.

**Example** `set last-member-query-interval = 10`

**Dependencies** The response time (the last-member-query-interval value divided by 10) must be less than the query-interval value.

**Location** `CONNECTION:ip-options:igmp-options`

## last-profile-sync

**Description** Read-only. Indicates the time at which the controller in this context last synchronized its profile repository with its partner.

**Usage** Read-only parameter with a numeric range of 0 to 4294967295.

**Example** `last-profile-sync = 123`

**Location** `REDUNDANCY-STATS:context-stats`

## last-reboot

**Description** Read-only. Indicates the reason the controller in this context was last rebooted.

**Usage** Read-only parameter with the following possible values:

- `crash`
- `local-report-local-error`
- `remote-report-local-error`
- `local-report-remote-error`
- `remote-report-remote-error`
- `local-manual-reboot`
- `remote-manual-reboot`
- `redundant-controller-switch-cmd`
- `number-of-reboot-types`
- `primary-operational-reboot`
- `secondary-operational-reboot`

**Example** `last-reboot = crash`

**Location** `REDUNDANCY-STATS:context-stats`

## last-received

**Description** Read-only. Indicates the time at which the controller in this context last received a redundancy message.

**Usage** Read-only parameter with a numeric range of 0 to 4294967295.

**Example** last-received = 123

**Location** REDUNDANCY-STATS:context-stats

## last-sent

**Description** Read-only. Indicates the time at which the controller in this context last got an acknowledgement (ACK) for a sent redundancy message.

**Usage** Read-only parameter with a numeric range of 0 to 4294967295.

**Example** last-sent = 123

**Location** REDUNDANCY-STATS:context-stats

## last-state-change

**Description** Reports the date and time (the real-time clock from the real-time clock from the control module) when the dev-line-state parameter is changed.

**Usage** Read-only. The output is recorded in the following format:  
{ { hour minute second } { Week Month Year Day } }

**Example** last-state-change = { { 15 34 42 } { Wednesday April 2004 14 } }

**Location** physical-status

## last-switch-time

**Description** Read-only. A time stamp that indicates the time since the last switchover to the other channel in automatic protection switching (APS). The TAOS timestamp shows the number of ticks since December 1, 1990.

**Usage** Valid values for this read-only parameter range from 0 through 2147483647.

**Example** last-switch-time = 3487821

**Location** APS-STAT

## leadership-priority

**Description** Specifies a number representing the leadership priority value that the node advertises to the peer group in a Private Network-to-Network Interface (PNNI).

**Usage** The default 0 (zero) value is required for nodes that are not peer group leader/logical group node (PGL/LGN) capable.

**Example** `set leadership-priority = 0`

**Location** `PNNI-NODE-CONFIG [n] :node-pgl`

## least-delay-link

**Description** Read-only. Indicates the index of the link configured in the inverse multiplexing over ATM (IMA) group which has the smallest link propagation delay.

**Usage** Valid range is from 0 (zero) to 24. A value of zero is used if no link has been configured in the IMA group, or if the link with the smallest link propagation delay has not yet been determined.

**Example** `least-delay-link = 0`

**Location** `IMA-GROUP-STAT`

## left-status

**Description** Specifies the default content of the left side of the status window.

**Usage** Valid values are as follows:

- `session-list`—Specifies that the Stinger unit displays current system administration sessions on the left side of the status window.
- `connection-list`—Specifies that the Stinger unit displays current system WAN sessions on the left side of the status window. This is the default.

**Example** `set left-status = session-list`

**Location** `USER`

## len

**Description** Specifies the number of bytes to test in a packet, starting with the byte specified by the `offset` parameter. The packet data is compared to the value setting specified in the filter. The `mask` setting is assumed to have the same number of octets as the data specified by the `len` parameter.

**Usage** Specify a number from 0 to 8. The default is 0 (zero), which indicates that no packet data is tested.

**Example** `set len = 8`

In this generic filter specification, the filter applies the mask to the 8 bytes following the specified offset.

**Dependencies** This setting applies only if the `type` parameter in the `input-filter` or `output-filter` subprofile is set to `generic-filter`.

**Location** `FILTER:input-filters [n] :gen-filter`  
`FILTER:output-filters [n] :gen-filter`

## length

**Description** Specifies the number of bytes in a specified address. Length is used in a specific way in each profile or subprofile

**Usage** Valid values are as follows:

- In the atm-addr-alias profile—Number of bytes in the aliased address (from 0 to 22 bytes).
- In the pnni-node-prefix subprofile of the atm-prefix profile—Length in number of bytes of the prefix portion of the Private Network-to-Network Interface (PNNI) node address. By default, the prefix is 13 bytes, which is consistent with the DCC-AESA format. The valid range is from 1 to 13.
- In the spvc-addr-prefix subprofile of the atm-prefix profile—Length in number of bytes of the prefix portion of the soft permanent virtual circuit (SPVC) target address. With the default (0) zero setting, the value is taken from the pnni-node-prefix profile's length setting. The valid range is from 0 to 13.
- In the svc-addr-prefix subprofile of the atm-prefix profile—Length in number of bytes of the prefix portion of the switched virtual circuit (SVC) interface address. With the default zero setting, the value is taken from the pnni-node-prefix profile's length setting. The valid range is from 0 to 13.

**Example** The following command sets the aliased address length in the atm-addr-alias profile:

```
set length = 22
```

**Location** ATM-ADDR-ALIAS  
ATM-PREFIX:pnni-node-prefix  
ATM-PREFIX:spvc-addr-prefix  
ATM-PREFIX:svc-addr-prefix

## lim-sparing-enabled

**Description** Specifies whether the line interface module (LIM) redundancy trap (notification) is sent to the identified host.

**Usage** Valid values are as follows:

- yes—Specifies that LIM redundancy trap is sent to the identified host.
- no—Specifies that LIM redundancy trap is not sent to the identified host. This is the default.

**Example** set lim-sparing-enabled = yes

**Dependencies** Only when this parameters is set to no can the Stinger unit report traps to an SNMP agent.

**Location** TRAP

## lim-status-ok

**Description** Read-only. Indicates the status of line interface module (LIM) redundancy for a given LIM.

**Usage** Valid values are as follows:

- `yes`—Indicates that the LIM redundancy for this port is properly working.
- `no`—Indicates that LIM redundancy for this port is not properly working.

**Example** `LIM-status-ok = no`

**Location** `LIM-SPARING-STATUS`

## linear-protection-channel

**Description** Specifies the physical address of a protection channel in automatic protection switching (APS).

**Usage** Specify a valid physical address for a trunk port in terms of shelf, slot, and port. The value `{ any-shelf any-slot 0 }` is invalid.

**Example** `set linear-protection-channel = { 1 trunk-module-1 2 }`

**Location** `APS-CONFIG`

## line-build-out

**Description** Specifies the line buildout value, in decibels, for connecting to channel service unit (CSU) devices.

**Usage** Valid values are as follows:

- `0-db`—This is the default.
- `7.5-db`
- `15-db`
- `22.55-db`

**Dependencies** For this setting to apply, you must set the Front-End-Type parameter to long-haul.

**Example** `set line-build-out = 15-db`

**Location** `DS1-ATM:line-config`

## line-code

**Description** Specifies the discrete multitone (DMT) line code to be used for training.

**Usage** Valid values are as follows:

- `auto-select`—Enables automatic detection of the ADSL line coding. This is the default value for any line interface module (LIM) except the ADSL 48-port G.lite LIM.
- `ansi-dmt`—Sets the line code to the ANSI DMT standard. Use this value for optimum performance when configuring a 12-port LIM to ANSI DMT.
- `g.lite`—Sets the line code to the G.lite standard. The line code is automatically set to this value for the ADSL 48-port G.lite LIM.
- `g.dmt`—Sets the line code to the G.dmt standard.
- `legacy-mode`—For 24-port ADSL LIMs only. Allows training to legacy Alcatel devices such as the CopperCom MXR integrated access device (IAD) modem.
- `etsi-annex-b`—For Annex B ADSL LIMs only. Sets European Telecommunications Standards Institute (ETSI) mode. ETSI mode uses a single tone to initiate the startup sequence and fixes the location of bins for upstream and downstream rates.

**Example** `set line-code = auto-select`

**Location** `AL-DMT:line-config`

## line-latency-down

**Description** Specifies the latency path for downstream data transport.

**Usage** Valid values are as follows. The default value is `interleave` for G.lite and `fast` for all other line codings.

- `fast`—Specifies noninterleaved channels.
- `interleave`—Specifies interleaved channels.

**Example** `set line-latency-down = fast`

**Dependencies** The `fast-path-config` subprofile values are not relevant to the 48-port line interface module (LIM) configuration because fast latency is not available for that configuration.

**Location** `AL-DMT:line-config`

## line-latency-up

**Description** Specifies the latency path for upstream data transport.

**Usage** Valid values are as follows. The default value is `interleave` for G.lite and `fast` for all other line codings.

- `fast`—Specifies noninterleaved channels.
- `interleave`—Specifies interleaved channels.

**Example** `set line-latency-up = fast`

**Dependencies** The `fast-path-config` subprofile values are not relevant to the 48-port line interface module (LIM) configuration because fast latency is not available for that configuration.

**Location** `AL-DMT:line-config`

## line-length

**Description** Specifies the length of the physical line in feet for connecting to short-haul digital cross-connect (DSX) devices.

**Usage** Valid values are as follows:

- 1-133—Equivalent to 0.3m to 40.5m. This is the default.
- 134-266—Equivalent to 40.8m to 81.1m.
- 267-399—Equivalent to 81.4m to 121.6m.
- 400-533—Equivalent to 121.9m to 162.5m.
- 534-655—Equivalent to 162.8m to 199.6m.

**Dependencies** This parameter replaces the `max-cable-loss` parameter in the `ds1-atm` profile. While the `line-length` and `max-cable-loss` parameters have the same valid values, you must reapply the value set in the `max-cable-loss` parameter to the `line-length` parameter for the setting to apply.



**Note** This parameter does not apply if the `front-end-type` parameter is set to `long-haul`.

**Example** `set line-length = 1-133`

**Location** `DS1-ATM:line-config`

## line-mode

**Description** Depending on the profile, indicates or specifies the mode in which this line is operating.

**Usage** Valid values are as follows:

- In the `ds1-atm-stat` profile, the following values are read-only:
  - `uni`—Indicates that the link operates in User-to-Network-Interface (UNI) mode.
  - `ima`—Indicates that the link operates in inverse multiplexing over ATM (IMA) mode.
- In the `line-config` subprofile of the `sds1` profile, specify one of the following values:
  - `atm`—Specifies that the line operates in Asynchronous Transfer Mode (ATM).
  - `hdlc`—Specifies that the line operates in High-Level Data Link Control (HDLC) serial mode.



**Example** Use the following examples to help you read or set line-mode:

- In the following example, the DS1 line mode is in UNI mode:  
line-mode = uni
- The following command sets an SDSL line to run in HDLC serial mode:  
set line-mode = hdlc

**Location** DS1-ATM-STAT  
SDSL:line-config

## line-quality

**Description** Read-only. Indicates the line quality (in decibels). For an SDSL interface, a reading of -5dB or better is required for reliable data transfer.

**Usage** The line-quality setting is read-only.

**Example** line-quality = 15

**Location** HDSL2-STAT:physical-statistic  
SDSL-STAT:physical-statistic  
SHDSL-STAT:physical-statistic

## line-rate

**Description** Read-only. Indicates the maximum data rate for this port.

**Usage** The line-rate setting is read-only.

**Example** line-rate = 148598

**Location** HIGH-SPEED-SLOT-STATIC-CONFIG:trunk-cac-config



**Note** This parameter was previously located in the atm-config profile. Its use in that location has been deprecated.

## line-state

**Description** Read-only. Indicates the overall state of a line.

**Usage** The line-state setting is read-only. You cannot set line-state directly. For a RADS L or an ADSL line, line-state can have one of the following values:

| Value    | Indicates                               |
|----------|-----------------------------------------|
| disabled | Line is disabled.                       |
| active   | Line is enabled and operating normally. |

For an SDSL, HDSL2, or an SHDSL line, *line-state* can have one of the following values:

| <b>Value</b>   | <b>Indicates</b>                        |
|----------------|-----------------------------------------|
| does-not-exist | Line is not installed.                  |
| disabled       | Line is disabled.                       |
| active         | Line is enabled and operating normally. |

For an IDSL line, *line-state* can have one of the following values:

| <b>Value</b>   | <b>Indicates</b>                    |
|----------------|-------------------------------------|
| disabled       | Line is disabled.                   |
| no-physical    | No physical link exists.            |
| point-to-point | Point-to-point link is established. |

For a DS3-ATM or an OC3-ATM line, *line-state* can have one of the following values:

| <b>Value</b>   | <b>Indicates</b>                                                                                       |
|----------------|--------------------------------------------------------------------------------------------------------|
| does-not-exist | No link is established.                                                                                |
| disabled       | Line is disabled.                                                                                      |
| loss-of-signal | Red Alarm state has occurred, which indicates a near-end loss of signal.                               |
| loss-of-frame  | Framing error has occurred on the near end.                                                            |
| yellow-alarm   | Device on the line is detecting framing errors in the signal, which indicates a far-end loss of frame. |
| ais-receive    | Line is receiving a keepalive signal.                                                                  |
| active         | Line is enabled.                                                                                       |

For a DS1-ATM line, *line-state* can have one of the following values:

| <b>Value</b>             | <b>Indicates</b>                                   |
|--------------------------|----------------------------------------------------|
| does-not-exist           | No link is established.                            |
| disabled                 | Line is disabled.                                  |
| loss-of-sync             | Red-alarm state, plus or minus.                    |
| yellow-alarm             | Yellow-alarm state.                                |
| ais-receive              | Receiving keep-alive signal.                       |
| loss-of-cell-delineation | ATM receiver is in loss of cell delineation state. |
| active                   | The line is active and operational.                |

**Example** line-state = active

**Location** AL-DMT-STAT

ATM-INTERNAL-STAT

DS1-ATM-STAT

DS3-ATM-STAT

E3-ATM-STAT

HDSL2-STAT

IDSL-STAT

OC3-ATM-STAT

SDSL-STAT

SHDSL-STAT

## line-up-timer

**Description** Read-only. Indicates the length of time the line has been in the UP state.

**Usage** The line-up-timer value is read-only. It has the following format:

{hh mm ss}

- *hh*—Indicates the number of hours.
- *mm*—Indicates the number of minutes.
- *ss*—Indicates the number of seconds.

**Location** AL-DMT-STAT:physical-statistic

HDSL2-STAT:physical-statistic

IDSL-STAT:physical-statistic

SDSL-STAT:physical-statistic

SHDSL-STAT:physical-statistic

## link-compression

**Description** Specifies the link-compression method for Point-to-Point Protocol (PPP)-encapsulated packets transmitted and received on the connection.

**Usage** Valid values are the following:

- *none*—Does not use link compression. This value is the default in the *answer-defaults* profile.
- *stac*—Uses a modified version of draft 0 of the Compression Control Protocol (CCP), which predates RFC 1974. This modified version is supported by older equipment. This value is the default in *connection* profiles.
- *stac-9* —Uses draft 9 of the Stac LZS compression protocol, which is described in RFC 1974. Most devices use this compression method.
- *ms-stac*—Uses Microsoft/Stac compression (the method used by Windows 95). If the caller does not acknowledge Microsoft/Stac compression, the Stinger unit attempts to use standard *stac* compression. If the caller does not acknowledge *stac* compression, the link uses no compression.
- *mppc*—Uses Microsoft Point-to-Point Compression (MPPC).

**Example** `set link-compression = stac-9`

**Dependencies** Both sides of the connection must support the same type of link compression. Otherwise, this setting has no effect.

**Location** `ANSWER-DEFAULTS:ppp-answer`  
`CONNECTION:ppp-options`

### linkdown-enabled

**Description** Specifies whether the system generates a trap when a failure occurs in a communication link between the unit and the SNMP manager.

**Usage** Valid values are as follows:

- `yes`—Specifies that the system generates a trap when a failure occurs in a communication link between the unit and the SNMP manager. This is the default.
- `no`—Specifies that the system does not generate a trap when a failure occurs in a communication link between the unit and the SNMP manager.

**Example** `set linkdown-enabled = no`

**Location** `TRAP`

### link-mgmt

**Description** Specifies the link management protocol between the Stinger unit and the frame relay switch. The frame relay administrator or service provider can tell you which value to use.



**Note** To ensure interoperability with equipment from different vendors, the same version of management protocol must be used at each end of the frame relay link.

**Usage** Valid values are as follows:

- `none`—Specifies no link management. The Stinger unit assumes that the physical link is enabled and that all Data Link Connection Indicators (DLCIs) are active on the physical link. This is the default.
- `ANSI-T1.617d`—Specifies the link management protocol defined in ANSI T1.617 Annex D.
- `CCITT-Q.933a`—Specifies the link management protocol defined Q.933 Annex A.

**Example** `set link-mgmt = ansi-t1.617d`

**Location** `FRAME-RELAY`

## link-mgmt-dlci

**Description** Specifies the data link connection identifier (DLCI) to use for link management on the frame relay data link.

**Usage** Specify one of the following settings:

- `dlci0` (the default)—Specifies DLCI 0.
- `dlci1023`—Specifies DLCI 1023.

**Example** `set link-mgmt-dlci = dlci1023`

**Dependencies** When switched virtual circuit (SVC) signaling is enabled, `link-mgmt-dlci` must be set to its default value of `dlci0`.

**Location** `FRAME-RELAY`

## link-recovery-type

**Description** Specifies the type of link recovery.

**Usage** Valid values are as follows:

- `manual`—Link recovery type is manual.
- `slow`—Link recovery type is slow.
- `fast` (the default)—Link recovery type is fast.

**Example** `set link-recovery-type = slow`

**Location** `DS1-ATM:line-config:ima-option-config:rxlink-config`  
`DS1-ATM:line-config:ima-option-config:txlink-config`

## link-state

**Description** Read-only. Indicates the physical state of the LAN interface.

**Usage** The `link-state` setting is read-only. The value can be set by the Ethernet driver only.

- `up`—Indicates that the LAN interface can transmit and receive network traffic.
- `down`—Indicates that the LAN interface cannot transmit and receive network traffic (for example, if the Ethernet cable is unplugged or the Ethernet hub on the interface is not operating).
- `unknown`—Indicates an Ethernet interface on the control module.

**Example** `link-state = up`

**Location** `ETHER-INFO`

## link-state-enabled

**Description** Specifies whether the link state of the Ethernet interface affects the system's IP routing tables.

**Usage** Valid values are as follows:

- **yes**—Specifies that the Stinger unit deletes routes to an interface when the interface is unavailable, and then restore the routes when the interface becomes available again.
- **no** (the default)—Specifies that the Stinger unit does not choose an alternate route if the interface is unavailable. (Packets are discarded.)

**Example** `set link-state-enabled = yes`

**Location** `ETHERNET`

## link-type

**Description** Specifies the kind of logical interface between the Stinger unit and the frame relay network on the data link:

- **Data circuit-terminating equipment (DCE)** is a device that connects the data terminal equipment (DTE) to a communications channel, such as a telephone line.
- **Data terminal equipment (DTE)** is a device that an operator uses, such as a computer or a terminal.
- **Network-to-Network Interface (NNI)** operation allows the Stinger unit to act as a frame relay switch communicating with another frame relay switch.

**Usage** Valid values are as follows:

- **dce**—Specifies a UNI-DCE connection. The Stinger unit operates as the network side, communicating with the user side (UNI-DTE) of a frame relay terminating unit.
- **dte**—Specifies a UNI-DTE connection. The Stinger unit operates as the user side, communicating with the network-side DCE switch. This is the default.
- **nni**—Specifies an NNI connection. The Stinger unit performs both DTE and DCE link management.

**Example** `set link-type = dce`

**Location** `FRAME-RELAY`

## linkup-enabled

**Description** Specifies whether the system generates a trap (notification) when the communication link between the unit and the SNMP manager is reestablished.

**Usage** Valid values are as follows:

- **yes**—Specifies that the system generates a trap when the communication link between the unit and the SNMP manager is reestablished. This is the default.
- **no**—Specifies that the system does not generate a trap when the communication link between the unit and the SNMP manager is reestablished.

**Example** `set linkup-enabled = no`

**Location** `TRAP`

## load-end

**Description** Read-only. Indicates the time at which the controller in this context detected that the other controller completed loading the operational code.

**Usage** Read-only parameter with a numeric range of 0 to 4294967295.

**Example** `load-end = 123`

**Location** `REDUNDANCY-STATS:context-stats`

## loadname

**Description** Read-only. Indicates the name of the software load that was running on a slot that failed.

**Usage** The `loadname` setting is read-only.

**Example** `loadname = load1`

**Location** `ERROR`

## load-start

**Description** Read-only. Indicates the time at which the controller in this context started waiting for the other controller to load the operational code.

**Usage** Read-only parameter with a numeric range of 0 to 4294967295.

**Location** `REDUNDANCY-STATS:context-stats`

## local

**Description** Read-only. Indicates the identity and reboot statistics for the controller in this context.

**Usage** Read-only, complex field.

**Example** `local = { 10486893 }`

**Location** `REDUNDANCY-STATS:context-stats`

### local-address

**Description** Specifies an IP address assigned to the local side of a numbered-interface connection. The Stinger unit uses this value to match the address presented by an incoming IP connection.

Bridged IP routing (BIR) configurations require numbered interfaces, for which the remote and local side of the connection are each assigned a unique IP address. Typically, the local address for the Stinger unit is a unique address on the remote subnet.

**Usage** Specify an IP address. The default is the null address (0.0.0.0/0).

**Example** `set local-address = 1.2.3.4/32`

**Dependencies** A numbered interface is required when BootP packets come from an interface that is not point-to-point.

**Location** `CONNECTION:ip-options`  
`CONNECTION:bir-options:multiple-ip-address:ip-address-option[n]`

### local-echo

**Description** *Not used.*

**Location** `TERMINAL-SERVER:terminal-mode-configuration:telnet-options`

### local-net

**Description** *Not used.* Read-only. Indicates the local-net number representing the highest level of the Private Network-to-Network Interface (PNNI) hierarchy that lies within the local network scope.

**Usage** The local-net value is read-only. Valid values range from 0 to 104. The default value is 96.

**Example** `local-net = 96`

**Location** `PNNI-NODE-CONFIG [n] :node-scope-mapping`



## local-net-plus-1

**Description** *Not used.* Indicates the local-net number representing the highest level of the Private Network-to-Network Interface (PNNI) hierarchy that lies within the local network plus 1 scope.

**Usage** The local-net-plus-1 value is read-only. Valid values range from 0 to 104. The default value is 96.

**Example** local-net-plus-1 = 96

**Usage** PNNI-NODE-CONFIG [n] :node-scope-mapping

## local-net-plus-2

**Description** *Not used.* Indicates the local-net number representing the highest level of the Private Network-to-Network Interface (PNNI) hierarchy that lies within the local network plus 2 scope.

**Usage** The local-net-plus-2 value is read-only. Valid values range from 0 to 104. The default value is 96.

**Example** local-net-plus-2 = 96

**Location** PNNI-NODE-CONFIG [n] :node-scope-mapping

## local-profiles-first

**Description** Specifies whether the Stinger unit attempts local authentication before remote external authentication.

**Usage** Specify one of the following settings:

- **lpf=yes** (the default)—Specifies that the Stinger unit first attempts to authenticate the connection with a local profile. If the profile exists and the password matches, the Stinger unit allows the connection. If no local profile exists or if a local profile exists but the password fails, the Stinger unit tries to authenticate the connection through an external authentication server.
- **lpf=no**—Specifies that the Stinger unit first tries to authenticate the connection through a remote authentication server. If the server acknowledges the request, it allows the connection. If the server does not acknowledge (NAKs) the request and remote authentication fails (because no remote profile exists, or a remote profile exists but the password fails), or if the remote authentication server cannot be reached, the Stinger unit attempts to authenticate the connection with a local profile.
- **lpf=mo**—Specifies that the Stinger unit first tries to authenticate the connection through a remote authentication server. If the profile exists and the password matches, the Stinger unit allows the connection. If the server does not respond, the Stinger unit checks for a matching local profile. If the server does not acknowledge (NAKs) the request and remote authentication fails, the Stinger unit terminates the connection.

**Example** set local-profiles-first = lpf=no

**Dependencies** Consider the following:

- If auth-type is set to none, local-profiles-first does not apply.
- PAP-Token authentication does not produce a challenge with a local profile. Using a local profile defeats the security of using PAP-Token.
- When you use a local profile, PAP-Token-CHAP brings up one channel, but all other channels fail.
- If the remote end of the connection has ever been authenticated with a challenge, Cache-Token does not work with a local profile. If the remote end has never been authenticated, no problem occurs when using a local profile.
- When you set local-profiles-first to lpf-no, the Stinger unit waits for the remote authentication to time out before attempting to authenticate locally. This time-out might take longer than the time-out specified for the connection and could cause all connection attempts to fail. Therefore, set the authentication time-out value low enough to guard against the line becoming unavailable, but high enough to permit the unit to respond if it can. The recommended time is 3 seconds.

**Location** EXTERNAL-AUTH

## location

**Description** Specifies the physical location of the Stinger unit or remote shelf. An SNMP manager can both read and set the location value in an SNMP profile.

**Usage** Specify text describing where the Stinger unit or remote shelf is located. You can enter up to 80 characters for a Stinger unit or 83 characters for a remote shelf. The default is null.

**Example** set location = building-64

**Location** SNMP  
REMOTE-SHELF-CONFIG

## log-call-progress

**Description** Specifies whether the unit logs incoming call-progress messages.

**Usage** Valid values are as follows:

- yes—Specifies that the unit logs incoming call-progress messages. This is the default.
- no—Specifies that the unit discards incoming call-progress messages.

**Example** set log-call-progress = no

**Location** LOG

## log-date

**Description** Date the command log was generated. This parameter reports date in the format { Weekday Month Year Date }.

**Usage** This parameter is read-only.

**Example** log-date = { Friday November 2003 7 }

**Location** cmd-log

## log-display-level

**Description** Specifies the lowest level of the log messages that the Stinger unit displays to a logged-in user.



**Note** Do not confuse log-display-level with save-level in the log profile. The save-level parameter determines which messages are displayed in the event-log status window.

**Usage** The following levels are arranged from the highest—starting with emergency—to the lowest, debug. Specify a level as the lowest level setting. The level you specify and all levels above that setting are displayed. For example, if critical is the lowest setting, only critical, alert, and emergency level log messages are displayed.

- none (the default)—The Stinger unit does not display log messages.
- emergency—The unit has an error condition and is unlikely to be operating normally.
- alert—The unit has an error condition but is still operating normally.
- critical—An interface has failed, or a security error has occurred.
- error—An error event has occurred.
- warning—An unusual event has occurred, but the unit is otherwise operating normally. For example, this type of message appears when a login attempt has failed because the user entered an incorrect username or password.
- notice—Events of interest in normal operation have occurred (a link becoming enabled or disabled, for example).
- info—State and status changes that are commonly not of general interest have occurred.
- debug—Helpful debugging information.

**Example** set log-display-level = debug

**Location** USER

## logical-item

**Description** Specifies a number that assigns an addressable logical entity within the context of a physical address.

**Usage** Specify a number from 0 (zero) to 2147483647.

**Example** `set logical-item = 0`

**Location** `CALL-ROUTE:preferred-source`

`CALL-ROUTE:index`

`REMOTE-SHELF-STAT:host-port`

`IP-INTERFACE:interface-address`

## login-level

**Description** Login level for a user profile.

**Usage** Specify one of the following values:

- `first-level` (the default)—This user profile is to be used for first level authentication.
- `second-level`—This user profile is to be used for second level authentication. If the `login-level` parameter is set to `second-level`, you must specify the name of a valid first-level user profile for the `first-level-user` parameter.

**Example** `set login-level = second-level`

**Location** `USER`

## login-prompt

**Description** *Not used.*

## login-source

**Description** Method used to initiate the user session.

**Usage** This parameter is read-only.

**Example** `login-source = console`

**Location** `cmd-log`

## login-timeout

**Description** *Not used.*

**Location** `TERMINAL-SERVER:terminal-mode-configuration`

## log-software-version

**Description** Specifies whether the Stinger unit logs the system version number.

**Usage** Valid values are as follows:

- `yes` (the default)—The system version number is logged.
- `no`—The system number is not logged.

**Example** set log-software-version = yes

**Location** LOG

## log-time

**Description** Time the command was entered, in the format { Hour Minute Second }.

**Usage** This parameter is read-only.

**Example** log-time = { 6 58 12 }

**Location** cmd-log

## loop-attenuation

**Description** Read-only. Indicates current diminution (attenuation) in the loop, in decibels (dB).

**Usage** This value is read-only.

**Example** loop-attenuation = 10

**Location** HDLSL2-STAT:physical-statistic  
SHDSL-STAT:physical-statistic

## loopback

**Description** Specifies whether to run a loopback test on the interface. While the interface is looped back, normal data traffic is interrupted.

**Usage** Valid values are as follows:

- no-loopback (the default)—Specifies that no loopback test is run.
- fe-loopback—Front-end loopback. Received data is transmitted back to the far-end by the transceiver at the near-end.
- line-loopback—Line loopback. The received data is looped back to the far-end without doing any re-framing of the T1/E1 frame.
- remote-loopback—Remote payload loopback. The received payload on the line is transmitted back to the far-end by reframing the payload at the near-end transmitter.
- local-loopback—Local loopback. The transmitted data is looped back to the near-end receiver by the local transceiver.

**Example** set loopback = local-loopback

**Location** DS1-ATM:line-config  
DS3-ATM:line-config  
E3-ATM:line-config  
OC3-ATM:line-config

## loop-back

**Description** Specifies whether the line passes normal data or is in loopback mode.

**Usage** Valid values are as follows:

- none (the default)—Specifies that no loopback test is run.
- analog—Specifies that the line is enabled for analog loopback tests. Terminating the DSL line with a 100-ohm resistor might be required.
- digital—Specifies that the line is enabled for digital loopback tests.

**Example** `set loop-back = digital`

**Location** AL-DMT:line-config  
HDSL2 :line-config  
SDSL:line-config  
SHDSL:line-config

## loopback-cells-per-test

**Description** Specifies the number of loopback-per-test cells to be sent on each ATM circuit to be tested.

**Usage** Specify a number from 1 through 10. The default is 1. The time interval between transmission of each loopback cell is 1 second.

**Example** `set loopback-cells-per-test = 5`

**Location** ATM-OAM:loopback-config

## loopback-level

**Description** Specifies the type of loopback test.

**Usage** Specify one of the following values:

- end-to-end—Specifies testing at the end-to-end level.
- segment (the default)—Specifies testing at the segment level.

**Example** `set loopback-level = end-to-end`

**Location** ATM-OAM:loopback-config

## loop-resistance

**Description** Read-only. Indicates the resistance, in ohms, registered in the loop during a copper loop test (CLT).

**Usage** The loop-resistance value is read-only.

**Example** `loop-resistance = 0`

**Location** CLT-RESULT

## loop-resistance-length-1

**Description** Read-only. Indicates the estimated length of resistance for 22 American wire gauge (AWG) or 0.644mm cable size.

**Usage** The loop-resistance-length-1 value is read-only. Valid values are as follows:

- If units are set to *english*, length-1 is the estimated length in hundredths of a foot (0.01) based on 22 AWG cable size.
- If units are set to *metric*, length-1 is the estimated length in centimeters based on a 0.644mm cable size.

**Example** loop-resistance-length-1 = 0

**Location** CLT-RESULT

## loop-resistance-length-2

**Description** Read-only. Indicates the estimated length of resistance for 24 American wire gauge (AWG) or 0.511mm cable size.

**Usage** The loop-resistance-length-2 value is read-only. Valid values are as follows:

- If units are set to *english*, length-2 is the estimated length in hundredths of a foot (0.01) based on 24 AWG cable.
- If units are set to *metric*, length-2 is the estimated length in centimeters based on 0.511mm cable size.

**Example** loop-resistance-length-2 = 0

**Location** CLT-RESULT

## loop-resistance-length-3

**Description** Read-only. Indicates the estimated length of resistance for 26 American wire gauge (AWG) or 0.405mm cable size.

**Usage** The loop-resistance-length-3 value is read-only. Valid values are as follows:

- If units are set to *english*, length-3 is the estimated length in hundredths of a foot (0.01) based on 26 AWG cable size.
- If units are set to *metric*, length-3 is the estimated length in centimeters based on 0.405mm cable size.

**Example** loop-resistance-length-3 = 0

**Location** CLT-RESULT

## loop-resistance-temp

**Description** Specifies the temperature of loop in a copper loop test (CLT).

**Usage** Specify a number according to the loop-resistance-unit value specified. Valid values are as follows:

- If loop-resistance-unit is english, specify a value in the range 0 to 100 degrees F.
- If loop-resistance-unit is metric, specify a value in the range -178 to 93.3 degrees C in tenths (0.1) of a degree.

**Example** set loop-resistance-temp = 80

**Dependencies** The loop-resistance-unit parameter must specify the type of units of measurement.

**Location** CLT-COMMAND

## loop-resistance-unit

**Description** Specifies the unit of measurement for the for loop resistance test in a copper loop test (CLT).

**Usage** Valid values are as follows:

- english—Uses English units for test parameters.
- metric (the default)—Uses metric units for test parameters.

**Example** set loop-resistance-unit = metric

**Dependencies** The loop-resistance-temp parameter must specify the temperature.

**Location** CLT-COMMAND

## loop-timing

**Description** Sets the source for transmission (TX) timing.

**Usage** Valid values are as follows:

- yes—Specifies that the TX timing for all the trunk ports, including this port, are derived from the receiver inputs of the port.
- no—Specifies that the TX timing is derived from the reference clock. This is the default.

**Example** set loop-timing = yes

**Location** OC3-ATM:line-config



## loss-detect-interval

**Description** Specifies the number of seconds between successive transmissions of Integrated Local Management Interface (ILMI) messages on this interface for the purpose of detecting loss of ILMI connectivity. *ILMI is not supported with the current software version.*

**Usage** Specify a value of from 0 to 65536 seconds. The default value is 5.

**Example** set loss-detect-interval = 25

**Dependencies** If this parameter is set to 0, ILMI connectivity procedures are disabled on the interface.

**Location** ATM-IF-CONFIG:extension-config

## loss-of-carrier

**Description** Read-only. Indicates a loss of carrier on the DS1 ATM line.

**Usage** Valid values are as follows:

- false—Indicates no loss of carrier.
- true—Indicates a loss of carrier.

**Example** loss-of-carrier = false

**Location** DS1-ATM-STAT  
T1-STAT

## loss-of-cell-delineation

**Description** Read-only. Indicates whether a header error control (HEC) check failed on the line.

**Usage** The loss-of-cell-delineation setting is read-only. Valid values are as follows:

- true—Indicates that an HEC check failed.
- false—Indicates that the line passed an HEC check.

**Example** loss-of-cell-delineation = false

**Location** OC3-ATM-STAT

## loss-of-frame

**Description** Read-only. Indicates whether a framing error has occurred on the line (also known as a *red alarm*).

**Usage** The Loss-Of-Frame value is read-only. Valid values are as follows:

- true—Indicates that a framing error has occurred on the line.
- false—Indicates that the line is operational and in frame.

**Example** loss-of-frame = false

**Location** DS3-ATM-STAT  
E3-ATM-STAT  
OC3-ATM-STAT

## loss-of-signal

**Description** Read-only. Indicates whether the carrier is maintaining a connection or not.

**Usage** The loss-of-signal value is read-only. Valid values are as follows:

- true—Indicates that the carrier is not maintaining a connection.
- false—Indicates that the carrier is maintaining a connection.

**Example** loss-of-signal = false

**Location** DS3-ATM-STAT  
E3-ATM-STAT  
OC3-ATM-STAT

## loss-of-sync

**Description** Read-only. Indicates a loss of synchronization on the DS1 ATM line.

**Usage** Valid values for this read-only parameter are as follows:

- true—Indicates a loss of synchronization.
- false—Indicates no loss is indicated.

**Example** loss-of-sync = false

**Location** DS1-ATM-STAT  
T1-STAT

## losw-second

**Description** Read-only. Indicates the number of 1-second intervals during which one or more HDLSL2 loss-of-synchronous-word (LOSW) defects are declared.

**Usage** The losw-second value is read-only.

**Example** losw-second = 1

**Location** HDLSL2-STAT: physical-statistic  
SHDSL-STAT: physical-statistic

## low-priority-weight

**Description** Sets the weight of this queue on the low-priority scheduler.

The relative weight determines how much of the scheduler's work cycle this queue can receive relative to other queues on the same scheduler.

**Usage** Specify a value in the range 0 to 15. The total weight per scheduler must be less than or equal to 128. The high-priority weight or low-priority weight must be nonzero if the queue is active.

**Example** `set low-priority-weight = 0`

**Location** SWITCH-CONFIG:atm-parameters:outgoing-queue

## lqm

**Description** Specifies whether the Stinger unit requests link-quality monitoring (LQM) when answering a PPP session request.

Link-quality monitoring counts the number of packets sent across the link and periodically queries the remote end about how many packets it has received. Discrepancies are evidence of packet loss and indicate link-quality problems. Link-quality monitoring also generates periodic link-quality reports, and the two ends of the link exchange the reports.

**Usage** Specify yes or no. The default is no.

- yes—Requests link-quality monitoring.
- no—Does not request link-quality monitoring.

**Example** `set lqm = yes`

**Location** ANSWER-DEFAULTS:ppp-answer  
CONNECTION:ppp-options

## lqm-maximum-period

**Description** Specifies the maximum period, in hundredths of a second, during which the Stinger unit can accept and send link-quality monitoring (LQM) packets when answering a PPP session request.

**Usage** Specify a number from 0 to 600. The default is 600.

**Example** `set lqm-maximum-period = 300`

**Dependencies** This setting does not apply if lqm is set to no.

**Location** ANSWER-DEFAULTS:ppp-answer  
CONNECTION:ppp-options

#### `lqm-minimum-period`

**Description** Specifies the minimum period, in hundredths of a second, during which the Stinger unit can accept link-quality monitoring (LQM) packets when answering a PPP session request.

**Usage** Specify a number from 0 to 600. The default is 600.

**Example** `set lqm-minimum-period = 200`

**Dependencies** This setting does not apply if `lqm` is set to `no`.

**Location** `ANSWER-DEFAULTS:ppp-answer`  
`CONNECTION:ppp-options`

## M

### mac-address

**Description** Specifies the media access control (MAC) address of an Ethernet interface.

An Ethernet MAC address is a 12-digit hexadecimal number denoting the physical address encoded in the controller.

**Usage** In most cases, the `mac-address` value is obtained from the system. However, you can clone a profile by reading an existing one and changing its physical address.

**Example** `set mac-address = 00:c0:6c:4e:ac:5a`

**Location** `ETHER-INFO`

### mac-address-learning-limit

**Description** Maximum number of MAC addresses the system will learn across the interface via transparent bridging. Address learning limits in `connection` profiles apply to all transparent bridging connections, which include both Ethernet and N:1 VLAN bridging.

**Usage** Specify a number. The default value is 16.

**Example** `set mac-address-learning-limit = 5`

**Location** `CONNECTION:bridging-options`

### mac-entry-age-time

**Description** Timeout interval (in seconds) at which the system ages out inactive MAC addresses from the bridge group's bridging table.

**Usage** Valid values are from 0 (which disables the address aging function) to 65535. The default value is 300.

**Example** `set mac-entry-age-time = 600`

**Dependencies** A maximum of 32K addresses can be aged out systemwide. If you modify this value for a bridge group that is in use, the new value is used for the next timeout.

**Location** `BRIDGE-GROUP`

**magic-key**

**Description** Read-only. *Parameter for internal use only.*

**Usage** The magic-key value is read-only.

**Example** magic-key = 358

**Location** ATMVCC-STAT

**magic-keys**

**Description** Read-only. *Parameter for internal use only.*

**Usage** The magic-key array values are read-only.

**Example** magic-keys[1] = 16777313

magic-keys[2] = 16777313

**Location** ATMPVC-STAT

**major-firmware-ver**

**Description** Read-only. Indicates the major firmware version of the SDSL line interface module (LIM).

**Usage** The major-firmware-ver value is read-only.

**Location** SDSL-STAT:physical-status

**management-only-interface**

**Description** Enables or disables management-only on the IP interface.

On a management-only interface, 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 on the management-only interface. Traffic generated externally is dropped on the interface.

**Usage** Valid values are as follows:

- yes—Terminates all incoming traffic received on the interface in the system itself, and transmit only traffic generated by the system itself.
- no (the default)—Processes inbound and outbound traffic normally on the interface.

**Example** set management-only-interface = yes

**Location** IP-INTERFACE

## manually-spared-slot-number

**Description** Specifies the slot number of the primary line interface module (LIM) associated with the spare LIM specified by the `spare-slot-number` parameter.

**Usage** Specify an integer. The default is `any-slot`.

**Example** `set manually-spared-slot-number = 2`

**Dependencies** The `manually-spared-slot-number` setting does not apply if `sparing-mode` is set to `inactive`.

**Location** `LIM-SPARING-CONFIG`

## margin

**Description** Specifies the noise margin value (in decibels) in the configuration of an HDDSL2 or SHDSL line.

**Usage** Specify a value from 0dB to 10dB, considering the following:

- Specifying a value *less than 6dB* causes modems to train at higher rates, but on noisy loops, modems might become unstable and retrain.
- Specifying a value *greater than 6dB* causes the modems to train at lower rates, but the modems are more stable and are less likely to retrain on noisy loops.

**Example** `set margin = 10db`

**Dependencies** This parameter applies only if the `interface-type` parameter is set to `g-shdsl` and the `rate-mode` parameter is set to `auto-mode`.

**Location** `HDDSL2:line-config`  
`SHDSL:line-config`

## marking-type

**Description** Enables or disables marking of packets to provide information for other network elements in a network domain using differentiated services code points (DSCPs).

Changing the value of this setting in a `connection` profile takes effect for new connections when the profile is written.

**Usage** Valid values are as follows:

- `precedence-tos` (the default)—Marks packets in a manner consistent with RFC 791, in which the first 6 bits in the second octet indicate the precedence and type of service (TOS) of the packet, as specified in the `precedence` and `type-of-service` settings.
- `dscp`—Marks packets as specified in RFC 2474, making use of the DSCP value specified in the `dscp` parameter.

**Example** `set marking-type = dscp`

**Dependencies** For this setting to apply, TOS and IP routing must be enabled in the connection profile, or TOS must be specified as the filter type in the filter profile.

**Location** CONNECTION:ip-options:tos-options  
 FILTER:input-filters[n]:tos-filter  
 FILTER:output-filters[n]:tos-filter  
 PACKET-FLOWS

## mask

**Description** Specifies a binary mask. The system applies the 12-byte mask to the value setting before comparing it to the packet data.

You can use the mask to specify exactly which bits you want to compare. The system translates both the mask and the value specified by the value parameter into binary format and then applies a logical AND operation to the results. Each binary 0 (zero) in the mask hides the bit in the corresponding position in the value. A mask of all ones (FF:FF:FF:FF:FF:FF:FF:FF) masks no bits, so the full specified value must match the packet contents.

**Usage** Specify a hexadecimal number of up to 12 bytes. The default is 000000000000.

**Example** set mask = 0f:ff:ff:ff:00:00:00:f0:00:00:00:00

**Dependencies** This setting applies only if the type parameter in the input-filter or output-filter subprofile is set to generic-filter.

**Location** FILTER:input-filters[n]:gen-filter  
 FILTER:output-filters[n]:gen-filter

## master-binding-port

**Description** Specifies whether an SHDSL port is configured for binding to the next adjacent port. Binding two SHDSL ports together aggregates their bandwidths together.

**Usage** Binding is enabled by configuring an odd numbered port as master. The next even numbered port is bound to the master port.

Specify one of the following values for master-binding-port parameter:

- no—Do not set the port to master binding port.
- yes—Set the port to master binding port.

**Dependencies** The rate-mode parameter must be set to fixed. The enabled parameter must be set to yes for both ports. The master port's max-rate and rate-mode parameter values are used for both ports.



**Note** The master-binding-port parameter is not active in the hdsl2:line-config profile.

**Location** HDLSL2:line-config  
 SHDSL:line-config



## match-method

**Description** Specifies how the context name specified in the incoming or outgoing protocol data unit (PDU) is to be matched to the value specified in the context-prefix parameter in the access-properties subprofile.

**Usage** Valid values are as follows:

- exact-match (the default)—Specifies that the entire context name specified in the incoming or outgoing PDU is to be matched to the value specified in the context-prefix parameter.
- prefix-match—Specifies that only the prefix of the context name specified in the incoming or outgoing PDU is to be matched.

**Example** set match-method = prefix-match

**Location** VACM-ACCESS

## max-active-vci-bits

**Description** Read-only. Indicates the maximum number of active virtual channel identifier (VCI) bits configured for use at this Asynchronous Transfer Mode (ATM) interface.

**Usage** This parameter is read-only.

**Example** max-active-vci-bits = 13

**Location** ATM-IF-CONFIG:base-config

## max-active-vpi-bits

**Description** Read-only. Indicates the maximum number of virtual path identifier (VPI) bits in virtual path identifier-virtual channel identifier (VPI-VCI) pairs on the asynchronous transfer mode ATM interface.

**Usage** This parameter is read-only.

**Example** max-active-vpi-bits = 8

**Location** ATM-IF-CONFIG:base-config

## max-add-noise-margin-down

**Description** Specifies the maximum downstream noise margin, in decibels beyond the target-noise-margin-down value, that the line tolerates relative to 0dB before attempting to reduce power output.

**Usage** Specify an integer from 0dB to 31dB. The default is 31dB for 12-port line interface modules (LIMs) and 30dB for 48-port LIMs.

For a system with typical noise patterns, set the max-add-noise-margin-down parameter to a value close to 8. For a system with greater noise patterns, you can set a higher value.

**Example** `set max-add-noise-margin-down = 15`

**Dependencies** Consider the following:

- You cannot set the `max-add-noise-margin-down` parameter to a value that is less than that of the `target-noise-margin-down` parameter.
- The modem software limits the maximum noise margin to 15dB. If you specify a setting greater than 15, the modem software uses 15dB.
- This parameter is not used for and has no effect on 24-port ADSL LIMS.

**Location** `AL-DMT:margin-config`

## `max-add-noise-margin-up`

**Description** Specifies the maximum upstream noise margin, in decibels beyond the `target-noise-margin-up` value, that the line tolerates relative to 0dB before attempting to reduce power output.

**Usage** Specify an integer from 0 to 31dB. The default is 31dB for 12-port line interface modules (LIMs) and 30dB for 48-port LIMs.

**Example** `set max-add-noise-margin-up = 15`

**Dependencies** Consider the following:

- You cannot set the `max-add-noise-margin-up` parameter to a value that is less than that of `target-noise-margin-up`.
- The modem software limits the maximum noise margin to 15dB. If you specify a setting greater than 15, the modem software uses 15dB.
- This parameter is not used for and has no effect on 24-port ADSL LIMS.

**Location** `AL-DMT:margin-config`

## `max-aggr-power-level-down`

**Description** Specifies the maximum aggregate power level on the downstream channel on the designated line in this `line-config` profile.

**Usage** Specify an integer from 0 to 20dBm. The default is 20

**Example** `set max-aggr-power-level-down = 13`

**Location** `AL-DMT:line-config`

## `max-aggr-power-level-up`

**Description** Specifies the maximum aggregate power level on the upstream channel on the designated line in this `line-config` profile.

**Usage** Specify an integer from 0 to 13dBm. The default is 13.

**Example** `set max-aggr-power-level-up = 10`

**Location** `AL-DMT:line-config`

## max-baud-rate

**Description** *Not used.*

**Location** `TERMINAL-SERVER:modem-configuration`

## max-bitrate-down

**Description** Specifies the maximum requested bit rate for downstream traffic.

**Usage** Specify an integer from 0Kbps to 15000Kbps. The default value is 8000Kbps.

**Example** `set max-bitrate-down = 10000`

**Dependencies** Consider the following:

- `max-bitrate-down` does not apply to operator-controlled rate-adaptation.
- If you set `max-bitrate-down` to a nonzero value in one of the subprofiles it appears in (either `fast-path-config` or `interleave-path-config`), set `max-bitrate-down` to 0 (zero) in the other subprofile.

**Location** `AL-DMT:fast-path-config`  
`AL-DMT:interleave-path-config`

## max-bitrate-up

**Description** Specifies the maximum requested bit rate for upstream traffic when operator-controlled rate-adaptive mode is in use.

**Usage** Specify an integer from 0Kpbs to 2000Kbps. The default value is 1000Kbps.

**Example** `set max-bitrate-up = 1200`

**Dependencies** Consider the following:

- `max-bitrate-up` does not apply to operator-controlled rate-adaptation.
- If you set `max-bitrate-up` to a nonzero value in one of the subprofiles it appears in (either `fast-path-config` or `interleave-path-config`), set `max-bitrate-up` to 0 (zero) in the other subprofile.

**Location** `AL-DMT:fast-path-config`  
`AL-DMT:interleave-path-config`

## max-bundle-members

**Description** Specifies the maximum number of data links allowed to join the multilink frame relay (MFR) bundle.

**Usage** Specify an integer. The default value is 1 (one). If you specify a number higher than 1, you can add bandwidth to the bundle up to the specified number of data links.

**Example** `set max-bundle-members = 4`

If `max-bundle-members` is set to 4 and the bundle has two data links, you can add bandwidth dynamically by configuring another data link profile with the bundle name.

**Dependencies** Consider the following:

- Because all member data links must reside on the same module, the module's capacity imposes a practical limitation on the maximum number of bundle members.
- The system checks first for a bundle specified by `mfr-bundle-name` in a connection profile. If it does not find a bundle name, it checks for one in the `frame-relay` profile.

**Location** `MULTI-LINK-FR`

## `max-burst-size`

**Description** Specifies the maximum number of Asynchronous Transfer Mode (ATM) cells that can be transmitted at peak cell rate (PCR) before the Stinger unit determines that the connection exceeds the traffic contract.

Once the maximum burst size (MBS) value is reached, the Stinger unit begins discarding or tagging cells.

**Usage** Specify a cell rate relative to the PCR, not a rate in kilobits per second. The range is 1 to 256. Default values are as follows:

- For the `atm-config` and `atm-internal` profiles, the default is 2.
- For the `atm-qos` profile, the default is 4.

**Example** `set max-burst-size = 10`

**Dependencies** The `max-burst-size` value applies only to variable bit rate (VBR) real-time traffic.

**Location** `SYSTEM:traffic-shapers`  
`ATM-INTERNAL:traffic-shapers [n]`  
`ATM-QOS`

## `max-call-duration`

**Description** Maximum number of minutes a session can stay connected.

**Usage** Specify a number from 0 through 1440. The default value of 0 (zero) sets no maximum limit on the duration of the session.

**Example** `set max-call-duration = 60`

**Location** `ANSWER-DEFAULTS:session-info`  
`CONNECTION:session-options`

**max-cc**

**Description** Specifies the maximum number of control protocol data unit (PDU) retransmissions of the types BGN, END, and RESYNC that are allowed.

**Usage** Valid values are from 0 (zero) to 64. The default value is 4 retransmissions allowed.

**Example** `set max-cc = 4`

**Location** ATM-IF-SIG-PARAMS:gsaal-options

**max-delay-down**

**Description** Specifies the maximum allowed downstream delay (in microseconds) that is induced by interleaving data.

**Usage** Specify a value from 0 to 64 microseconds. The default is 16.

**Example** `set max-delay-down = 10`

**Location** AL-DMT:interleave-path-config

**max-delay-up**

**Description** Specifies the maximum allowed upstream delay (in microseconds) that is induced by interleaving data.

**Usage** Specify a value from 0 to 64 microseconds. The default is 16.

**Example** `set max-delay-up = 10`

**Location** AL-DMT:interleave-path-config

**max-dialout-time**

**Description** *Not used.*

**Location** SYSTEM

**maximum-channels**

**Description** Specifies the default value for the maximum number of channels in a multichannel call.

**Usage** Specify a number from 1 to 32. The default is 2.

**Example** `set maximum-channels = 10`

**Location** CONNECTION:mp-options

## maximum-login-attempts

**Description** Maximum of number of login attempts that an administrative user can make.

**Usage** Specify a number between 1 through 6. The default value is 3.

**Example** `set maximum-login-attempts = 4`

**Location** SYSTEM

## maxlink-client-enabled

**Description** Read-only. Indicates whether the MAXLink client software is enabled.

**Usage** Valid values for this read-only parameter are as follows:

- `enabled`—Indicates that the MAXLink client software is enabled for the Stinger unit.
- `disabled`—Indicates that the MAXLink client software is not enabled.

**Example** `maxlink-client-enabled = enabled`

**Location** BASE

## max-margin-enabled

**Description** Enables or disables the ability of the Stinger unit to reduce the amount of transmit power according to the existing line conditions.

**Usage** Valid values are as follows:

- `yes`—Enables maximum power management.
- `no` (the default)—Disables maximum power management.

**Example** `set max-margin-enabled = yes`

**Dependencies** The system uses this parameter with the `max-add-noise-margin-down` and `max-add-noise-margin-down` parameters.

**Location** AL-DMT:margin-config

## max-pap-auth-retry

**Description** Specifies the maximum number of retries for failed Password Authentication Protocol (PAP) authentication attempts.

**Usage** Specify a number from 0 to 5. The default is 0 (zero).

**Example** `set max-pap-auth-retry = 3`

**Location** ANSWER-DEFAULTS:ppp-answer  
CONNECTION:ppp-options

## max-pd

**Description** Specifies the maximum number of sequenced data protocol data units (PDUs) allowed between poll intervals.

**Usage** Valid values are from 1 to 64. The default value is 25.

**Example** `set max-pd = 28`

**Location** ATM-IF-SIG-PARAMS:qsaal-options

## max-power-spectral-density

**Description** Specifies the maximum power spectral density (PSD) in both directions.

**Usage** Specify a number from 34 to 52 in even-numbered increments. The default is 40. If you specify an odd number, the system uses the even-numbered setting below it. The actual value used is the negative value of the number you specify.

**Example** `set max-power-spectral-density = 34`

**Location** AL-DMT:line-config

## max-rate

**Description** Specifies the maximum rate that the modem trains when `rate-mode` is set to `auto` in a configured HDSL2, SDSL or SHDSL line.

When `rate-mode` is set to `fixed`, the modem attempts to train only to the rate specified by this parameter. You need only to configure the central office equipment (COE) for the maximum rate value. The modem uses G.hs handshake protocol to communicate the maximum rate value to the customer premises equipment (CPE).

**Usage** Specify one of the following values in kilobits per seconds (Kbps):

- 72000
- 136000
- 200000
- 264000
- 328000
- 392000
- 456000
- 520000
- 584000
- 648000
- 712000
- 776000
- 840000
- 904000

- 968000
- 1032000
- 1096000
- 1160000
- 1224000
- 1288000
- 1352000
- 1416000
- 1480000
- 1544000
- 1608000
- 1672000
- 1736000
- 1800000
- 1864000
- 1928000
- 1992000
- 2056000
- 2120000
- 2184000
- 2248000
- 2312000
- 2320000

**Example** `set max-rate = 1544000`

**Dependencies** This parameter applies only if the `interface-type` parameter is set to `g-shdsl`.

**Location** HDLSL2:line-config  
SDSL:line-config  
SHDSL:line-config

## `max-restart`

**Description** Specifies the maximum number of unacknowledged transmit Restart messages allowed.

**Usage** Specify a number from zero (0) to 32. The default is 2.

**Example** `set max-restart = 4`

**Location** ATM-IF-SIG-PARAMS:q2931-options



## max-rip-trigger-delay

**Description** Specifies the maximum delay for triggered Routing Information Protocol (RIP) updates.

**Usage** Specify a value in seconds in a range from 1 to 30 seconds. The default is 8 seconds.

**Example** `set max-rip-trigger-delay = 20`

**Location** IP-GLOBAL

## max-shared-users

**Description** Specifies the maximum number of users that can be simultaneously connected through a shared profile.

**Usage** Enter a number from 0 (zero) to the maximum number of calls the system can handle. The default zero value indicates no limit on the number of users sharing a profile at the same time.

**Example** `set max-shared-users = 3`

**Location** CONNECTION

## max-source-port

**Description** Specifies the highest rlogin source port value.

**Usage** Specify an integer from 128 to 1023. The default is 1023.

**Example** `set max-source-port = 250`

**Dependencies** Consider the following:

- The max-source-port value must be greater than or equal to the setting of min-source-port.
- rlogin must be enabled for max-source-port to have any effect.

**Location** `TERMINAL-SERVER:terminal-mode-configuration:rlogin-options`

## max-stat

**Description** Specifies the maximum length of the STAT protocol data unit (PDU).

**Usage** Valid values are from 32 to 128. The default value is 67.

**Example** `set max-stat = 64`

**Location** `ATM-IF-SIG-PARAMS:qsaal-options`

**max-statenq**

**Description** Specifies the maximum number of unacknowledged transmit STATUS ENQ messages allowed.

**Usage** The default value is 1. Up to 32 are allowed.

**Example** `set max-statenq = 2`

**Location** ATM-IF-SIG-PARAMS:q2931-options

**max-switched-vcc-vpi**

**Description** Maximum number of virtual path identifiers (VPIs) supported by the signaling stack on the interface for allocation to switched virtual channel connections (SVCCs).

**Usage** The default value for Stinger units is 255. On a Private Network-to-Network Interface (PNNI)-enabled trunk interface, you can specify a lower number to restrict SVCCs to a lower range of VPIs on the interface.

**Example** `set max-switched-vcc-vpi = 128`

**Dependencies** This parameter can be modified only for trunk interfaces. If you change its value on a line interface module (LIM) interface, the system displays an error message and reverts to the default setting.

**Location** ATM-IF-CONFIG:extension-config

**max-switched-vpc-vpi**

**Description** Maximum number of virtual path identifiers (VPIs) supported by the signaling stack on the interface for allocation to switched virtual path connections (SVPCs).

**Usage** The default value for Stinger units is 255. On a PNNI-enabled trunk interface, you can specify a lower number to restrict SVCCs to a lower range of VPIs on the interface.

**Example** `set max-switched-vpc-vpi = 255`

**Dependencies** This parameter can be modified only for trunk interfaces. If you change its value on a line interface module (LIM) interface, the system displays an error message and reverts to the default setting.

**Location** ATM-IF-CONFIG:extension-config

## max-tunnels

**Description** In an Ascend Tunnel Management Protocol (ATMP) Home Agent gateway profile, specifies the maximum number of mobile clients that can use the connection, all at the same time, to tunnel into the home network.

**Usage** Specify an number from 0 through 65535. The default value of 0 (zero) sets no limit.

**Example** `set max-tunnels = 256`

**Dependencies** This setting applies only when profile-type specifies gateway-profile.

**Location** CONNECTION:tunnel-options

## max-upstream-bandwidth

**Description** Read-only. Indicates the maximum upstream bandwidth of all line interface modules (LIMs).

**Usage** The max-upstream-bandwidth value is read-only.

**Example** `max-upstream-bandwidth = 622160`

**Location** BANDWIDTH-STATS

## max-vccs

**Description** Read-only. Indicates the maximum number of virtual channel connections (VCCs) supported on the interface.

**Usage** This parameter is read-only.

**Example** `max-vccs = 8192`

**Location** ATM-IF-CONFIG:base-config

## max-vpcs

**Description** Read-only. Indicates the maximum number of virtual path connections (VPCs) supported on the interface.

**Usage** This parameter is read-only.

**Example** `max-vpcs = 255`

**Location** ATM-IF-CONFIG:base-config

**max-warning-core-dump**

**Description** Specifies the maximum value for a range of warning numbers that will generate a core dump.

**Usage** Specify a numeric value with range of to 9999. The default value is 0 (zero).

**Example** set max-warning-core-dump = 200

**Dependencies** Consider the following:

- enable-core-dump must equal yes for this parameter to be active.
- If min-warning-core-dump and max-warning-core-dump both equal 0 then only warnings from 101 to 121 will cause a core dump.

**Location** DEBUG

**mbone-lan-interface**

**Description** *Deprecated and not used.*

**Location** IP-GLOBAL

**See Also** IP-GLOBAL:multiple-mbone:mbone-lan-interface [n]

**mbone-lan-interface [n]**

**Description** An array of four indexed parameters which specifies the physical address (shelf, slot, and port) of a LAN interface used to reach a multicast backbone (MBONE) router.

**Usage** Specify the physical interface address of an Ethernet interface on which the MBONE router resides.

**Example** set mbone-lan-interface[1] physical-address = { { 1 3 0 } 0 }

**Dependencies** This parameter and the mbone-profile[n] parameter are mutually exclusive.

**Location** IP-GLOBAL:multiple-mbone

**mbone-profile**

**Description** Specifies the name of a local connection profile for a multicast backbone (MBONE) router on a WAN interface.

**Usage** Specify the station name of a connection profile to the MBONE router.

**Example** set mbone-profile = wan3-mbone

**Dependencies** This parameter and the mbone-lan-interface parameter are mutually exclusive.

**Location** IP-GLOBAL

## `mbone-profile [n]`

**Description** An array of four indexed parameters which specifies the name of a local connection profile for a multicast backbone (MBONE) router on a WAN interface.

**Usage** Specify the station name of a connection profile to the MBONE router.

**Example** `set mbone-profile[1] = wan3-mbone`

**Dependencies** This parameter and the `mbone-lan-interface[n]` parameter are mutually exclusive.

**Location** `IP-GLOBAL:multiple-mbone`

## `mcast-ip-address`

**Description** IP address of a multicast group.

**Usage** Specify the IP address of a valid multicast group. The default is 0.0.0.0.

**Example** `set mcast-ip-address = 192.10.122.11`

**Location** `MCAST-SERVICE:filter-list [n]`

## `mcast-monitor-enabled`

**Description** Enables or disables the multicast monitor trap.

**Usage** Select one of the following values:

- `no`—Disable the multicast monitor trap.
- `yes`—Enable the multicast monitor trap. This is the default.

**Example** `set mcast-monitor-enabled = no`

**Location** `TRAP`

## `mcast-type`

**Description** Specifies the connection topology type.

**Usage** Specify one of the following values:

- `p2p`—The connection is a point-to-point connection. This is the default.
- `p2mproot`—The host is the root of point-to-multipoint connection.
- `p2mpleaf`—The host is a leaf of point-to-multipoint connection.

**Example** `set mcast-type = p2mproot`

**Location** `ATM-VCL-CONFIG`  
`ATM-VPL-CONF`

#### md5-authen-key

**Description** Specifies the secret key to be used for the message-digest algorithm 5 (MD5) cryptographic authentication method for Open Shortest Path First (OSPF) virtual links.

**Usage** Specify a text string of up to 16 characters. The default value is `ascend0`.

**Example** `set md5-authen-key = 12!secret*34key`

**Dependencies** When `authen-type` is set to `md5`, you must supply a value for the `md5-authen-key` setting, because the `auth-key` value no longer applies.

**Location** `OSPF-VIRTUAL-LINK`

#### md5-auth-key

**Description** Specifies the secret key to be used for the Open Shortest Path First (OSPF) message-digest algorithm 5 (MD5) cryptographic authentication method.

**Usage** Specify a text string of up to 16 characters. The default value is `ascend0`.

**Example** `set md5-auth-key = 12!secret*34key`

**Dependencies** When `authen-type` is set to `md5`, you must supply a value for the `md5-auth-key` setting, because the `auth-key` value no longer applies.

**Location** `CONNECTION:ip-options:ospf-options`  
`IP-INTERFACE:ospf`

#### media-speed-mbit

**Description** Specifies the operating speed of the Ethernet interface.

**Usage** Valid values are as follows:

- `100mb` (the default)—Sets the interface speed to 100Mbps.
- `10mb`—Sets the interface speed to 10Mbps.

**Example** `set media-speed-mbit = 10mb`

**Dependencies** The system can determine the proper setting for this parameter when `auto-negotiate` is set to `yes`.

**Location** `ETHERNET`

#### menu-selection-string

**Description** *Not used.*

**Location** `TERMINAL-SERVER:menu-mode`

## metric

**Description** Specifies a RIP-style metric for the route.

RIP is a distance-vector protocol that uses hop count as its metric. Among routes with the same destination address, a higher metric means that the system is less likely to choose the route.

**Usage** Specify a number from 0 to 15. In an `ip-route` profile, the default is 8. In a `private-route-table` profile, the default is 0.

**Example** `set metric = 3`

**Location** `IP-ROUTE`  
`PRIVATE-ROUTE-TABLE:route-description-list [n]`

## metrics1

**Description** *Not used.* Specifies the maximum cell rate in cells per second for the service categories represented in the `metrics-classes` value.

**Usage** The default value is 4294967295 (0xFFFFFFFF).

**Example** `set metrics1 = 4294967295`

**Location** `PNNI-METRICS`

## metrics2

**Description** *Not used.* Specifies the available cell rate in cells per second for the service categories represented in the `metrics-classes` value.

**Usage** The default value is 4294967295 (0xFFFFFFFF).

**Example** `set metrics2 = 4294967295`

**Location** `PNNI-METRICS`

## metrics3

**Description** *Not used.* Specifies the cumulative maximum cell transfer delay in microseconds for the service categories represented in the `metrics-classes` value.

**Usage** The default value is 4294967295 (0xFFFFFFFF).

**Example** `set metrics3 = 4294967295`

**Location** `PNNI-METRICS`

## metrics4

**Description** *Not used.* Specifies the cumulative cell delay variation in microseconds for the service categories represented in the metrics-classes value.

**Usage** The default value is 4294967295 (0xFFFFFFFF).

**Example** `set metrics4 = 4294967295`

**Location** PNNI-METRICS

## metrics5

**Description** *Not used.* Specifies the cumulative cell loss ratio for traffic having a cell loss priority (CLP) of 0 (zero), for the specified service categories.

**Usage** The Stinger unit computes the cell-loss ratio value as  $10^{**}(-n)$  where n is the value returned in this variable. The default value is 4294967295 (0xFFFFFFFF).

**Example** `set metrics5 = 4294967295`

**Location** PNNI-METRICS

## metrics6

**Description** *Not used.* Specifies the cumulative cell loss ratio for traffic having a cell loss priority (CLP) of 0+1, for the specified service categories.

**Usage** The Stinger unit computes the cell loss ratio value as  $10^{**}(-n)$  where n is the value returned in this variable. The default value is 4294967295 (0xFFFFFFFF).

**Example** `metrics6 = 4294967295`

**Location** PNNI-METRICS

## metrics7

**Description** *Not used.* Specifies the cell rate margin in cells per second for the service categories represented in the metrics-classes value.

**Usage** The default value is 4294967295 (0xFFFFFFFF).

**Example** `metrics7 = 4294967295`

**Location** PNNI-METRICS

## metrics8

**Description** *Not used.* Specifies the variance factor in units of  $2^{**}(-8)$  for the service categories represented in the metrics-classes value.

**Usage** The default value is 4294967295 (0xFFFFFFFF).



**Example** `metrics8 = 4294967295`

**Location** `PNNI-METRICS`

## `metrics-admin-weight`

**Description** Specifies the relative weight of the service categories assigned in the `pnni-metrics` profile, from the advertising node to the remote end of a Private Network-to-Network Interface (PNNI) link.

The lower the weight, the higher the preference for using the link. Weight can be assigned for any reason significant to the network administrator, but it is not intended to express information such as bandwidth capacity, which is provided by other values.

**Usage** Specify a number between 1 and 2,147,483,647, assigning the relative weight. The default value is 5040.

**Example** `set metrics-admin-weight = 5040`

**Location** `PNNI-METRICS`

## `metrics-classes`

**Description** Specifies a number that translates to a 5-bit binary bit mask representing the service category or categories to which this set of metrics applies.

Each bit that is set represents a single service category for which the resources indicated are available:

- Bit 5 represents constant bit rate (CBR).
- Bit 4 represents real-time variable bit rate (VBR).
- Bit 3 represents nonreal-time VBR.
- Bit 2 represents available bit rate (ABR).
- Bit 1 represents unspecified bit rate (UBR).

**Usage** Specify a decimal integer that translates to a binary bit mask representing a service category. The 0 (zero) default indicates that the metrics do not apply to the associated service categories. A 1 (one) value indicates that the metrics do apply.

**Example** Use the following examples to help you:

- The following example sets a value that translates to the binary number 11111, which indicates that the specified metrics apply to all service categories:  
`set metrics-classes = 31`
- The following example sets a value that translates to binary 10000, which indicates that the metrics apply to CBR traffic only:  
`set metrics-classes = 16`

**Location** `PNNI-METRICS`

## metrics-direction

**Description** Specifies the direction in which the parameters in this profile apply, relative to the advertising node.

**Usage** Valid values are as follows:

- `incoming` (the default)—Metrics apply to traffic coming into the advertising node.
- `outgoing`—Metrics apply to traffic leaving the advertising node.

**Example** `set metrics-direction = outgoing`

**Location** `PNNI-METRICS:metrics-index`

## metrics-gcac-clp

**Description** Specifies the cell loss priority (CLP) level at which the advertised generic connection admission control (GCAC) parameters apply.

**Usage** Valid values are as follows:

- `clpequal0or1`—Specifies that GCAC parameters apply to cells with a cell loss priority of 1 (low-priority cells). Thus cells with a low priority can be discarded during periods of congestion. This is the default.
- `clpequal0`—Specifies that GCAC parameters apply to cells with a cell loss priority of 0 (normal cells). Thus normal priority cells can be discarded during periods of congestion.

**Example** `set metrics-gcac-clp = clpequal0`

**Location** `PNNI-METRICS`

## metrics-index

**Description** Specifies an integer used as an index into the set of parameters associated with `metrics-tag` and `metrics-direction`.

**Usage** Specify a number as the index. The default is 0 (zero).

**Example** `set metrics-index = 29`

**Location** `PNNI-METRICS:metrics-index`

## metrics-tag

**Description** Specifies an integer used to associate a set of traffic parameters that are always advertised together. This tag represents the group of metric settings that apply to the connectivity from the advertising node to the reachable address prefix.

**Usage** The tag must be defined in one or more `pnni-metrics` profiles. If no traffic parameters apply, use the default value 0 (zero).

**Example** `set metrics-tag = 12`

**Location** PNNI-METRICS:metrics-index  
PNNI-ROUTE-ADDR

## mfr-bundle-name

**Description** Specifies the name of the multilink frame relay (MFR) bundle to which this data link belongs.

**Usage** Specify a string of up to 15 characters. This name is used differently according to the profile in which it occurs:

- In a multi-link-fr profile, mfr-bundle-name defines a name for the bundle and for the Multi-Link-FR profile.
- In a frame-relay profile—mfr-bundle-name adds the data link and all data link connection identifiers (DLCIs) that use it to the MFR bundle. All member data links must specify the same bundle name in the frame-relay profile.
- In a connection profile—mfr-bundle-name adds the DLCI.

**Example** `set mfr-bundle-name = mfrb1`

**Location** CONNECTION:fr-options  
FRAME-RELAY  
MULTI-LINK-FR

## mfr-bundle-type

**Description** Specifies the type of multilink frame relay (MFR) configuration.

**Usage** Only the mfr-dte type is supported.

**Example** `set mfr-bundle-type = mfr-dte`

**Location** MULTI-LINK-FR

## min-bandwidth

**Description** Specifies the minimum aggregated bandwidth before a multilink frame relay (MFR) bundle is considered inactive.

**Usage** Accept the default of 0 (zero). Because of an unresolved problem in frame relay, if min-bandwidth is set to any other value, data is not sent on the bundle.

**Example** `set min-bandwidth = 0`

**Location** MULTI-LINK-FR

## min-bitrate-down

**Description** Specifies the minimum bit rate for downstream traffic.

**Usage** Specify an integer from 0 to 8192Kbps. The default value is 128Kbps.

**Example** `set min-bitrate-down = 100`

**Dependencies** Consider the following:

- When automatic rate-adaptive mode is in effect, the line initializes at the downstream rate of min-bitrate-down, or it does not initialize at all.
- min-bitrate-down does not apply to operator-controlled rate-adaptation.
- If you set min-bitrate-down to a nonzero value in one subprofile, min-bitrate-down must be set to 0 (zero) in the other subprofile.

**Location** AL-DMT:fast-path-config

AL-DMT:interleave-path-config

## min-bitrate-up

**Description** Specifies the minimum bit rate for upstream traffic.

**Usage** Specify an integer from 0 to 1024Kbps. The default value is 128Kbps.

**Example** `set min-bitrate-up = 20`

**Dependencies** Consider the following:

- When automatic rate-adaptive mode is in effect, the line initializes at the upstream rate of min-bitrate-up, or it does not initialize at all.
- min-bitrate-up does not apply to operator-controlled rate-adaptation.
- If you set min-bitrate-up to a nonzero value in one subprofile, set min-bitrate-up to 0 (zero) in the other subprofile.

**Location** AL-DMT:fast-path-config

AL-DMT:interleave-path-config

## minimum-cell-rate-cells-per-sec

**Description** Indicates the minimum cell rate (MCR).

**Usage** This field is valid only for SPVC connections in a PNNI network. MCR for pseudo-ABR service, expressed in cells per second. The default value is 37 CPS, with a valid range from 0 to 353207 CPS. The value of this field is user-writable only if the system profile atm-qos-rate-unit parameter is set to cps.

**Example** `set minimum-cell-rate-cells-per-sec = 200`

**Location** ATM-QOS

## minimum-channels

**Description** Specifies the minimum number of channels in a multichannel call.

**Usage** Specify an integer from 1 to 32. The default is 1.

**Example** `set minimum-channels = 2`

**Location** `ANSWER-DEFAULTS:mp-answer`  
`CONNECTION:mp-options`

## `minimum-rate-kbits-per-sec`

**Description** Indicates the minimum bit rate in kilobits per second.

**Usage** This field is valid only for SPVC connections in a PNNI network. Minimum cell rate (MCR) for pseudo-ABR service, expressed in kilobits per second. The default value is 16Kbps, with a valid range from 0 to 149760Kbps. The value of this field is user-writable only if the system profile `atm-qos-rate-unit` parameter is set to `kbps`.

**Example** `set minimum-rate-kbits-per-sec = 32`

**Location** `ATM-QOS`

## `min-noise-margin-down`

**Description** Specifies the minimum downstream noise margin that the line tolerates relative to 0dB before attempting to increase power output.

**Usage** Specify an integer from 1dB to 31dB. The default is 6dB for 12-port line interface modules (LIMs) and 0dB for 48-port LIMs.

**Example** `set min-noise-margin-down = 15`

**Dependencies** Consider the following:

- The modem software limits the maximum noise margin to 15dB. If you specify a setting greater than 15, the modem software uses 15dB.
- This parameter is not used for and has no effect on 24-port LIMs.

**Location** `AL-DMT:margin-config`

## `min-noise-margin-up`

**Description** Specifies the minimum upstream noise margin that the line tolerates relative to 0dB before attempting to increase power output.

**Usage** Specify an integer from 1 to 31dB. The default is 6dB for 12-port LIMs and 0dB for 48-port LIMs.

**Example** `set min-noise-margin-up = 15`

**Dependencies** Consider the following:

- The modem software limits the maximum noise margin to 15dB. If you specify a setting greater than 15, the modem software uses 15dB.
- This parameter is not used for and has no effect on 24-port LIMs.

**Location** `AL-DMT:margin-config`

**minor-firmware-ver**

**Description** Read-only. Indicates the minor firmware version of the synchronous digital subscriber line (SDSL) line interface module (LIM).

**Usage** The minor-firmware-ver setting is read-only.

**Example** minor-firmware-ver = 0

**Location** SDSL-STAT:physical-status

**min-rate**

**Description** Specifies the minimum rate in kilobits per second at which a modem trains when the rate-mode parameter is set to auto.

**Usage** Valid values are as follows:

- 72000 (default)
- 136000
- 200000
- 264000
- 328000
- 392000
- 456000
- 520000
- 584000
- 648000
- 712000
- 776000
- 840000
- 904000
- 968000
- 1032000
- 1096000
- 1160000
- 1224000
- 1288000
- 1352000
- 1416000
- 1480000
- 1544000
- 1608000
- 1672000
- 1736000

- 1800000
- 1864000
- 1928000
- 1992000
- 2056000
- 2120000
- 2184000
- 2248000
- 2312000
- 2320000

**Example** `set min-rate = 136000`

**Dependencies** This parameter applies to only if the `interface-type` parameter is set to `g-shdsl`.

**Location** `HDSL2:line-config`  
`SHDSL:line-config`

## `min-rip-trigger-delay`

**Description** Specifies the minimum delay, in seconds, for triggered Routing Information Protocol (RIP) updates.

**Usage** Specify a value in the range from 1 to 30 seconds. The default is 5 seconds.

**Example** `set min-rip-trigger-delay = 20`

**Location** `IP-GLOBAL`

## `min-source-port`

**Description** *Not used.*

**Location** `TERMINAL-SERVER:terminal-mode-configuration:rlogin-options`

## `min-switched-vcc-vci`

**Description** Specifies the minimum virtual channel identifier (VCI) supported by the signaling stack on the interface for allocation to switched virtual channel connections (SVCCs).

**Usage** The default value for Stinger units is 32. On a Private Network-to-Network Interface (PNNI)-enabled trunk interface, you can specify a higher number to restrict SVCCs to a smaller range of VCIs on the interface.

**Example** `set min-switched-vcc-vci = 128`

**Dependencies** This parameter can be modified only for trunk interfaces. If you change its value on a line interface module (LIM) interface, the system displays an error message and reverts to the default setting.

**Location** ATM-IF-CONFIG:extension-config

### `min-warning-core-dump`

**Description** Specifies the minimum value for a range of warning numbers that will generate a core dump.

**Usage** Specify a numeric value with range of to 9999. The default value is 0.

**Example** `set min-warning-core-dump = 200`

**Dependencies** Consider the following:

- `enable-core-dump` must equal yes for this parameter to be active.
- If `min-warning-core-dump` and `max-warning-core-dump` both equal 0, then only warnings from 101 to 121 will cause a core dump.

**Location** DEBUG

### `modem-failure-threshold`

**Description** Specifies the number of modems on this line interface module (LIM) that must be regarded as nonfunctional before this LIM is considered nonfunctional.

**Usage** Specify a number between 1 and 12. The default value is 12 modems.

**Example** `set modem-failure-threshold = 10`

**Location** LIM-SPARING-CONFIG:auto-lim-sparing-config:lim-sparing-config[n]

### `modem-hw-state`

**Description** Read-only. Indicates the state of the interface after initialization.

**Usage** The Modem-Hw-State value is read-only. Valid values are

- `init-ok` (the default)—Indicates that the interface is functioning normally.
- `bad-sdram`—Indicates memory problems, probably associated with a self-test failure.
- `bad-cache`—Indicates memory problems, probably associated with a self-test failure.
- `bad-cache-sdram`—Indicates memory problems, probably associated with a self-test failure.

**Example** `modem-hw-state = init-ok`

**Location** AL-DMT-STAT:physical-status



## mode-mismatch-clear-timer-duration

**Description** Specifies the mode mismatch clear timer duration in tens of milliseconds in automatic protection switching (APS).

**Usage** Specify a number from 0 through 4,294,967,295. The default is 1000.

**Example** set mode-mismatch-clear-timer-duration = 2000

**Location** APS-CONFIG

## mode-mismatch-failure

**Description** Read-only. Indicates whether a mode mismatch has occurred.

**Usage** Valid values for this read-only parameter are as follows:

- true—A revertive or nonrevertive mode mismatch occurred.
- false—No mode mismatch occurred.

**Example** mode-mismatch-failure = false

**Location** APS-STAT

## mode-mismatch-failure-timer-duration

**Description** Specifies the mode mismatch failure timer duration in tens of milliseconds in automatic protection switching (APS).

**Usage** Specify a number from 0 through 4,294,967,295. The default is 250.

**Example** set mode-mismatch-failure-timer-duration = 300

**Location** APS-CONFIG

## modem-mod

**Description** *Not used.*

**Location** TERMINAL-SERVER:modem configuration

## modem-table-index

**Description** Read-only. Indicates the Simple Network Management Protocol (SNMP) modem table index number of the device whose state is described by the admin-state or admin-state-phys-if profile.

**Usage** The modem-table-index setting is read-only.

**Example** modem-table-index = 0

**Location** ADMIN-STATE  
ADMIN-STATE-PHYS-IF

## modem-transmit-level

**Description** *Not used.*

**Location** `TERMINAL-SERVER:modem-configuration`

## mru

**Description** Specifies the maximum number of bytes the Stinger unit can receive in a single packet.

**Usage** In most cases, you can accept the default setting for the connection. If you must change the default, specify a value less than the default value.

- For PPP, the default is 1524. Accept the default unless the device at the remote end of the link cannot support it.
- For frame relay, the default is 1532.

**Example** `set mru = 1524`

**Location** `ANSWER-DEFAULTS:ppp-answer`  
`CONNECTION:ppp-options`  
`FRAME-RELAY`

## msg-proc-model

**Description** Specifies the message-processing model to use when generating SNMP messages.

**Usage** Specify one of the following values:

- v1 (the default)—Specifies SNMP version 1.
- v3—Specifies SNMP version 3. For SNMPv3 notifications support, specify v3.

**Example** `set msg-proc-model = v3`

**Location** `SNMPV3-TARGET-PARAM`

## mtu

**Description** Specifies the maximum transmission unit (MTU) size—the maximum number of bytes that the Stinger unit can send in a single packet.

**Usage** Specify a number from 128 to 1524 bytes. Defaults are as follows:

- For Point-to-Point Protocol (PPP) connections, the default is 1524.
- For Asynchronous Transfer Mode (ATM) connections, the default is 1560.

**Example** `set mtu = 1500`

**Location** `ANSWER-DEFAULTS:ppp-answer`  
`CONNECTION:atm-connect-options`  
`CONNECTION:atm-options`  
`CONNECTION:ppp-options`

## mtu-limit

**Description** Specifies the maximum IP packet size, in bytes, that the system can transmit to a remote agent without performing prefragmentation.

**Usage** Specify a number from 0 through 65535. The default value of 0 (zero) disables this feature. If you specify a nonzero value, the smallest IP packet size the system uses is 68, even if a smaller size is specified. This value complies with the minimum IP packet size requirement in RFC 791.

**Example** `set mtu-limit = 1472`

**Location** `ATMP`

## multicast-address

**Description** Specifies the multicast destination address for multicast stacking control packets. The packets are sent to the specified multicast address and to the UDP port number specified by `udp-port`.

**Usage** Specify an IP address in dotted decimal notation. The default setting is 239.192.74.72, which is within the organization local scope defined in RFC 2365 as the address space from which an organization must allocate subranges when defining scopes for private use.

The specified address must be a valid multicast (class D) address.

**Example** `set multicast-address = 239.192.74.75`

**Location** `STACKING`

## multicast-allowed

**Description** Enables or disables handling of Internet Group Management Protocol (IGMP) requests and responses on the LAN or WAN interface.

**Usage** Valid values are as follows:

- `yes`—Responds to IGMP client requests and responses.
- `no` (the default)—Does not respond to multicast clients on the interface.

**Example** `set multicast-allowed = yes`

**Dependencies** If you set `multicast-allowed` to `yes` and `multicast-rate-limit` remains at the default of 100, the Stinger unit handles IGMP responses and requests on the interface but does not forward multicast traffic. You must set `multicast-rate-limit` to a nondefault value before the Stinger unit can forward multicast traffic.

**Location** `CONNECTION:ip-options`  
`IP-INTERFACE`

## multicast-forwarding

**Description** Enables or disables multicast forwarding in the Stinger unit.

When you change the value to `yes` and write the profile, the multicast subsystem reads the values in the `ip-global` profile and initiates the forwarding function on the interface on which the multicast backbone (MBONE) router resides.

**Usage** Specify `yes` or `no`. The default is `no`.

- `yes`—Enables multicast forwarding.
- `no` (the default)—Disables multicast forwarding.

**Example** `set multicast-forwarding = yes`

**Dependencies** You must specify the interface on which the MBONE router resides by setting the `mbone-lan-interface` or `mbone-profile` parameters. If you modify a multicast value in the `ip-global` profile, you must toggle this setting to force a read of the new values.

**Location** `IP-GLOBAL`

## multicast-group-leave-delay

**Description** Specifies the number of seconds the Stinger unit waits before forwarding an Internet Group Management Protocol (IGMP)-v2 Leave Group message from a multicast client to the multicast backbone (MBONE) router.

**Usage** Specify a number of seconds from 0 to 120. The default is 0 (zero).

- If you accept the default, the Stinger unit forwards a Leave Group message immediately.
- If you specify a value other than the default, and the Stinger unit receives a Leave Group message, the unit sends an IGMP query to the WAN interface or client from which it received the Leave Group message. If the Stinger unit does not receive a response from an active multicast client that belongs to the client group, it sends a Leave Group message when the time you specify expires.

If users might establish multiple multicast sessions for identical groups, specify a value of 10 to 20 seconds.

**Example** `set multicast-group-leave-delay = 15`

**Dependencies** This setting applies only when `multicast-forwarding` and `multicast-allowed` are set to `yes`.

**Location** `CONNECTION:ip-options`  
`IP-INTERFACE`

## multicast-hbeat-addr

**Description** Specifies the multicast address to be monitored for determining a minimal level of traffic (heartbeat).

The heartbeat monitoring function causes the unit to poll for multicast traffic and, if desired, send an SNMP alarm if traffic falls below a certain threshold.

**Usage** Specify a multicast address in dotted decimal notation. The default is 0.0.0.0.

**Example** `set multicast-hbeat-addr = 224.1.1.4`

**Dependencies** All the `multicast-hbeat` values interact to enable the optional heartbeat monitoring feature and fine-tune multicast heartbeat monitoring.

**Location** IP-GLOBAL

## multicast-hbeat-alarm-threshold

**Description** Specifies the number of packets within the monitoring interval that represents normal multicast traffic. If the number of monitored packets falls below this number, the SNMP alarm trap is sent.

**Usage** Specify a number of packets that represents a minimal level of normal multicast traffic. The default value of 0 (zero) disables heartbeat monitoring.

**Example** `set multicast-hbeat-alarm-threshold = 100`

**Dependencies** All the `multicast-hbeat` values interact to enable the optional heartbeat monitoring feature and fine-tune multicast heartbeat monitoring.

For example, if you set `multicast-hbeat-number-slot` to 5, and `multicast-hbeat-slot-time` to 3 seconds, the Stinger unit polls five times at 3-second intervals. After 60 seconds of elapsed time, it compares the number of multicast packets received to the value of this parameter.

**Location** IP-GLOBAL

## multicast-hbeat-number-slot

**Description** Specifies the number of times to poll for the specified interval before comparing the number of heartbeat packets received to the alarm threshold.

**Usage** Specify the number of times the Stinger unit polls for packets before comparing to the threshold. The default is 0 (zero).

**Example** `set multicast-hbeat-number-slot = 5`

**Dependencies** All the multicast-hbeat values interact to enable the optional heartbeat monitoring feature and fine-tune multicast heartbeat monitoring.

For example, if you set multicast-hbeat-number-slot to 5, and multicast-hbeat-slot-time to 3 seconds, the Stinger unit polls five times at 3-second intervals. After 60 seconds of elapsed time, it compares the number of multicast packets received to the value of multicast-hbeat-alarm-threshold.

**Location** IP-GLOBAL

## multicast-hbeat-port

**Description** Specifies a UDP port number to be monitored for determining a minimal level of traffic (heartbeat). The Stinger unit counts only packets received on this port.

**Usage** Specify a UDP port number. The default is 0 (zero).

**Example** set multicast-hbeat-port = 16834

**Dependencies** All the multicast-hbeat values interact to enable the optional heartbeat monitoring feature and fine-tune multicast heartbeat monitoring.

**Location** IP-GLOBAL

## multicast-hbeat-slot-time

**Description** Specifies a polling interval (in seconds) during which the Stinger unit polls for multicast traffic.

**Usage** Specify the number of seconds between polling cycles. The default is 0 (zero).

**Example** set multicast-hbeat-slot-time = 6

**Dependencies** All the multicast-hbeat values interact to enable the optional heartbeat monitoring feature and fine-tune how multicast heartbeat monitoring operates.

For example, if you set multicast-hbeat-number-slot to 5, and multicast-hbeat-slot-time to 3 seconds, the Stinger unit polls five times at 3-second intervals. After 60 seconds of elapsed time, it compares the number of multicast packets received to the value of this parameter.

**Location** IP-GLOBAL

## multicast-hbeat-src-addr

**Description** Specifies a source IP address to be ignored. Packets received from that address are ignored for heartbeat monitoring purposes.

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

**Example** set multicast-hbeat-src-addr = 2.2.2.2

**Dependencies** All the multicast-hbeat values interact to enable the optional heartbeat monitoring feature and fine-tune multicast heartbeat monitoring.

**Location** IP-GLOBAL

## multicast-hbeat-src-addr-mask

**Description** Specifies a subnet mask that the system applies to the multicast-hbeat-src-addr value before comparing it to the source address in a packet.

**Usage** Specify a subnet mask. The default is 0.0.0.0.

**Example** set multicast-hbeat-src-addr-mask = 255.255.255.248

**Dependencies** All the multicast-hbeat values interact to enable the optional heartbeat monitoring feature and fine-tune multicast heartbeat monitoring.

**Location** IP-GLOBAL

## multicast-interface-ip-address

**Description** Specifies the IP address of the Ethernet port to be used for stacking IP multicast control traffic.

**Usage** Specify an IP address in dotted decimal notation. The default is 0.0.0.0, which specifies that the unit uses the system's shelf-controller Ethernet interface.

**Example** set multicast-interface-ip-address = 10.10.10.1

**Location** STACKING

## multicast-max-groups

**Description** Maximum number of links to multicast groups allowed for this client.

**Usage** Specify a numeric value between 0 and 512. The default is 0.

**Example** set multicast-max-groups = 4

**Location** CONNECTION:ip-options

## multicast-member-timeout

**Description** *Deprecated and not used.*

**Location** IP-GLOBAL

**See Also** CONNECTION:igmp-option

## multicast-rate-limit

**Description** Specifies the rate at which the Stinger unit accepts multicast packets from clients on the LAN or WAN interface.

**Usage** Valid values are as follows:

- To begin forwarding multicast traffic on the interface, specify an integer lower than 100.
- To disable the forwarding of multicast traffic on the interface, specify the default (100). This setting can help the multicast forwarder to prevent multicast clients from creating response storms to multicast transmissions. It does not affect the multicast backbone (MBONE) interface.

**Example** Setting this parameter as in the following example enables the Stinger unit to accept a packet from multicast clients on the interface every 5 seconds. The unit discards any subsequent packets received in that 5-second window .

```
set multicast-rate-limit = 5
```

**Dependencies** If you set `multicast-allowed` to `yes` and `multicast-rate-limit` remains at the default of 100, the Stinger unit handles Internet Group Management Protocol (IGMP) responses and requests on the interface but does not forward multicast traffic. You must set `multicast-rate-limit` to a nondefault value before the Stinger unit can forward multicast traffic.

**Location** CONNECTION:ip-options  
IP-INTERFACE

## multicast-server-vc

**Description** Specifies whether the virtual circuit IS a multicast server VC.

**Usage** Valid values are as follows:

- `yes`—The virtual circuit acts as an MBONE for IGMP joins coming from the DSL side, and the system forwards multicast traffic from the multicast server VC to DSL clients who have joined the group. However, IGMP control messages are not exchanged on the interface. The `encapsulation-protocol` parameter must be set to `atm`.
- `no`— Disables the feature. This is the default value.

**Example** `set multicast-server-vc = yes`

**Dependencies** The `multiple-multicast-server-vc` parameter in the `ip-global` profile must be set to `yes`.

**Location** CONNECTION:ip-options



## multicast-service-profile

**Description** *Deprecated.* Name of the mcast-service profile used by the client defined in the connection profile.

**Usage** Specify an alphanumeric value up to 31 characters long. The default value is null.

**Example** `set multicast-service-profile = gold`

**Location** CONNECTION:ip-options

**See Also** multiple-mcast-filter

## multiple-multicast-server-vc

**Description** Enables or disables the multicast server VC feature systemwide.

**Usage** Valid values are as follows:

- **yes**—Configure up to 100 trunk PVCs Stinger to receive multicast data from one multicast group.
- **no**—Disables the multicast server VC feature systemwide. This is the default value.

**Example** `set multiple-multicast-server-vc = yes`

**Dependencies** When this parameter is set to yes, you cannot configure MBONE or PIM.

**Location** IP-GLOBAL

## multi-rate-enabled

**Description** Read-only. Indicates whether the unit can make dialable wideband service (DWS) calls.

**Usage** The value is read-only. Valid values are as follows.

- **yes**—Indicates that the unit can make DWS calls.
- **no**—Indicates that the unit cannot make DWS calls.

**Example** `multi-rate-enabled = yes`

**Location** BASE

**must-accept-address-assign**

**Description** Enables or disables the ability of an incoming caller to reject an assigned IP address during PPP negotiation.

**Usage** Valid values are as follows:

- **yes**—Callers must accept assigned addresses. If a caller rejects dynamic IP address assignment, the Stinger unit hangs up.
- **no** (the default)—An address received from the far end can override a dynamically assigned address.

**Example** `set must-accept-address-assign = yes`

**Location** `IP-GLOBAL`

**must-agree**

**Description** Specifies whether the controllers must agree on the choice of a primary control module.

**Usage** Valid values are as follows:

- **no** (the default)—Specifies that the primary controllers need not agree on the choice of a primary control module. This setting enables a control module to become primary without the agreement of the other control module. This setting is recommended.
- **yes**—Specifies that the primary controllers must agree.

**Example** `set must-agree = no`

**Location** `REDUNDANCY:context:context [n]`

## N

### n391-val

**Description** Specifies the number of T391 polling cycles between full Status Enquiry messages.

**Usage** Specify an integer from 1 to 255. The default is 6, which specifies that after six status requests spaced t391-val seconds apart, the User-to-Network Interface for data circuit-terminating equipment (UNI-DTE) device requests a full status report.

**Example** set n391-val = 15

**Dependencies** If link-type is set to dce, n391-val does not apply.

**Location** FRAME-RELAY

### n392-val

**Description** Specifies the number of errors, during DTE-N393-monitored events, that cause the user side to declare the network side's procedures inactive.

**Usage** Specify an integer from 1 to 10. The value you enter must be less than the n393-val setting. The default is 3.

**Example** set n392-val = 5

**Dependencies** If link-type is set to dce, n392-val does not apply.

**Location** FRAME-RELAY

### n393-val

**Description** Specifies the DTE-monitored event count.

**Usage** Specify an integer from 1 to 10. The value you enter must be greater than the n392-val setting. The default is 4.

**Example** set n393-val = 6

**Dependencies** If link-type is set to dce, n393-val does not apply.

**Location** FRAME-RELAY

## nailed-group

**Description** For all profiles except the status profiles, specifies a number associated with the bandwidth of a physical interface. For atm-if-stat and ima-group-stat, this parameter indicates that number.

You refer to this number in a connection or RADIUS profile to bind the connection to the interface. The system generates a default nailed-group number for all Asynchronous Transfer Mode (ATM) interfaces of its external line and trunk modules, and for the internal ATM interface of an ISDN digital subscriber line (IDSL) or router module.

This parameter appears in every profile associated with a physical interface installed in the system. In all profiles in which it appears, except atm-if-stat and ima-group-stat, you can assign a different nailed-group number if necessary by modifying the value of this parameter.

**Usage** Specify a number from 1 to 2048, or use the default value assigned by the system.

**Example** set nailed-group = 200

**Dependencies** A nailed-group number must be unique within the system.

**Location** AL-DMT:line config  
 ATM-IF-STAT  
 ATM-INTERNAL:line-config  
 CONNECTION:atm-options  
 CONNECTION:atm-connect-options  
 DS1-ATM:line-config  
 DS3-ATM:line-config  
 OC3-ATM:line-config  
 E3-ATM:line-config  
 HDLSL2:line-config  
 IMAGROUP  
 IMA-GROUP-STAT  
 SDSL:line-config  
 SHDSL:line-config

## nailed-groups

**Description** *Not supported.* Specifies the nailed-group number for bandwidth used by the connection. Bandwidth is associated with specific connections in Stinger units in the atm-options and atm-connect-options subprofiles of a connection profile.

**Location** CONNECTION:telco-options

## nailed-mode

**Description** *Not used.* Specifies how the Stinger unit uses the link's dedicated (nailed-up) channels, and whether the link uses dedicated channels alone or a combination of dedicated and switched channels.

**Usage** Valid values are as follows:

- `ft1` (the default)—Specifies that the link uses only dedicated channels.
- `ft1-mpp`—Specifies that the link uses a combination of dedicated and switched channels.
- `ft1-bo`—Specifies that the link uses a combination of dedicated and switched channels with backup and overflow.

In providing backup bandwidth, the Stinger unit drops all the dedicated channels when the quality of a dedicated channel falls to Marginal or Poor in an FT1-BO call. The unit then attempts to replace dropped dedicated channels with switched channels. It also monitors dropped dedicated channels. When the quality of all dropped channels changes to Fair or Good, the unit reinstates them.

In providing overflow protection, the Stinger unit supplies supplemental dial-up bandwidth during times of peak demand to prevent saturation of a dedicated line. The circuit remains in place until the traffic subsides, and then it is removed.

**Example** `set nailed-mode = ft1`

**Location** `FRAME-RELAY`

## nailed-up-group

**Description** Specifies the group number assigned to the dedicated (nailed-up) channels of a frame relay link.

**Usage** Specify a number assigned to a group of dedicated channels. The maximum value you can enter is 1024. Default values are as follows:

- In a `connection` or `frame-relay` profile, the default is 1 (one).
- In a `call-info` profile, the default is 852.

**Example** `set nailed-up-group = 5`

**Location** `CALL-INFO`  
`CONNECTION:telco-options`  
`FRAME-RELAY`

name

**Description** Specifies a name for the configuration or other entity. If the name field indexes the profile, it is used by the system to retrieve the related configuration. If it is not used as the profile index, name is used for administrative purposes, or to specify the name of an outside entity such as a host or a user allowed to access the unit's interface.

For profiles that configure a physical interface, the system assigns a default name that shows a shorthand version of the interface physical address. For example, if the interface is in slot 4, interface 12, the system-generated name value is 1:4:12. However, you can replace this value with another name if you wish.

**Usage** Specify a text string that does not contain spaces. The maximum length and default value of name depend on the profile in which it is located, as shown in the following table:

| Profile location of name parameter                         | Maximum length | Default         |
|------------------------------------------------------------|----------------|-----------------|
| AL-DMT/{ any-shelf any-slot 0 }                            | 15 characters  | Null string     |
| ADSL-BIN-LOADING/""                                        | 23 characters  | Null string     |
| ALARM/""                                                   | 23 characters  | Null string     |
| APS-CONFIG/""                                              | 15 characters  | Null string     |
| APS-STAT/""                                                | 15 characters  | Null string     |
| ATM-INTERNAL/{ any-shelf any-slot 0 }                      | 15 characters  | Null string     |
| DS1-ATM/{ any-shelf any-slot 0 }                           | 15 characters  | shelf:slot:item |
| DS3-ATM/{ any-shelf any-slot 0 }                           | 15 characters  | Null string     |
| DSL-THRESHOLD/""                                           | 23 characters  | Null string     |
| E3-ATM/{ any-shelf any-slot 0 }                            | 15 characters  | Null string     |
| FLOW-SERVICES/""                                           | 31 characters  | Null string     |
| HDSL2/{ any-shelf any-slot 0 }                             | 15 characters  | Null string     |
| HIGH-SPEED-SLOT-STATIC-CONFIG/<br>{ any-shelf any-slot 0 } | 15 characters  | Null string     |
| IDSL/{ any-shelf any-slot 0 }                              | 15 characters  | Null string     |
| IMA-GROUP-STAT/""                                          | 15 characters  | Null string     |
| IMAGROUP/""                                                | 15 characters  | Null string     |
| IMAHW-CONFIG/{ any-shelf any-slot 0 }                      | 15 characters  | Null string     |
| IP-ROUTE/""                                                | 31 characters  | Null string     |
| OC3-ATM/{ any-shelf any-slot 0 }                           | 15 characters  | Null string     |
| PACKET-FLOWS/""                                            | 31 characters  | Null string     |
| PNNI-ROUTE-ADDR/""                                         | 50 characters  | Null string     |
| PRIVATE-ROUTE-TABLE/""                                     | 23 characters  | Null string     |
| REMOTE-SHELF-CONFIG                                        | 23 characters  | Null string     |
| SDSL/{ any-shelf any-slot 0 }                              | 15 characters  | Null string     |

| Profile location of <code>name</code> parameter         | Maximum length | Default                |
|---------------------------------------------------------|----------------|------------------------|
| SHDSL/{ any-shelf any-slot 0 }                          | 15 characters  | Null string            |
| SLOT-STATIC-CONFIG/<br>{ any-shelf any-slot 0 }         | 15 characters  | Null string            |
| SNMP-MANAGER/""                                         | 31 characters  | Null string            |
| SNMPV3-NOTIFICATION/""                                  | 23 characters  | Null string            |
| SNMPV3-TARGET-PARAM/""                                  | 23 characters  | Null string            |
| SNMPV3-USM-USER/""                                      | 23 characters  | Null string            |
| SWITCH-CONFIG/"" :atm-parameters:<br>outgoing-queue [n] | 15 characters  | <i>shelf:slot:item</i> |
| SYSTEM                                                  | 23 characters  | Null string            |
| USER/""                                                 | 23 characters  | Null string            |
| VRROUTER/""                                             | 23 characters  | Null string            |

**Example** set name = queue-originate

**Location** See preceding table.

## nas-port-type

**Description** *Not supported.* Specifies a type of service for the session.

**Location** CONNECTION:telco-options

## near-end-crc

**Description** Read-only. Indicates the number of cyclic redundancy check (CRC) errors detected by an ADSL transceiver unit (ATU) in the central office equipment (COE).

**Usage** The near-end-crc value is read-only.

**Example** near-end-crc = 0

**Location** AL-DMT-STAT:physical-statistic

## near-end-fec

**Description** Read-only. Indicates the number of forward error correction (FEC) errors detected by an ADSL transceiver unit (ATU) in the central office equipment (COE).

**Usage** The near-end-fec value is read-only.

**Example** near-end-fec = 0

**Location** AL-DMT-STAT:physical-statistic

## near-end-hec

**Description** Read-only. Indicates the number of header error checksum (HEC) errors detected by an ADSL transceiver unit (ATU) in the central office equipment (COE).

**Usage** The near-end-hec value is read-only.

**Example** near-end-hec = 0

**Location** AL-DMT-STAT:physical-statistic

## near-end-ima-group-state

**Description** Read-only. Indicates the current operational state of the near-end inverse multiplexing over ATM (IMA) group.

**Usage** Values are as follows:

| Value                         | Description                                                                                                                   |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| not-configured                | IMA group is not configured.                                                                                                  |
| start-up                      | IMA group is in the startup state.                                                                                            |
| start-up-ack                  | IMA group is in a transitional state and has transitioned out of IMA startup state.                                           |
| aborted-unsupported-framelenh | IMA group establishment failed because the frame length (M) received from the remote end was not acceptable to the local end. |
| aborted-incompatible-symmetry | IMA group establishment failed because the remote end and local end have incompatible group symmetry modes.                   |
| aborted-other                 | IMA group establishment failed for unspecified reasons.                                                                       |
| insufficient-links            | IMA group is currently in the insufficient links state.                                                                       |
| blocked                       | IMA group is in the blocked state.                                                                                            |
| operational                   | IMA group is in the operational state.                                                                                        |
| aborted-unsupported-version   | IMA group failed because of an IMA version mismatch between the local and remote ends.                                        |

**Example** near-end-ima-group-state = operational

**Location** IMA-GROUP-STAT



## near-end-num-failures

**Description** Read-only. Indicates the number of times a near-end group failure (for example, Config-Aborted or Insufficient-Links) has been reported in the current 15-minute interval.

**Usage** The valid range for this read-only value is from 0 (zero) to 2147483647.

**Example** near-end-num-failures = 3

**Location** IMA-GROUP-STAT:ima-group-statistic

## near-end-rx-failure-status

**Description** Read-only. Indicates the link's near-end receive (Rx) failure status.

**Usage** Valid values for this read-only parameter are as follows:

| Value                    | Description                                                                  |
|--------------------------|------------------------------------------------------------------------------|
| no-failure               | Link does not have any failure.                                              |
| ima-link-failure         | Link experienced a failure at the inverse multiplexing over ATM (IMA) layer. |
| lif-failure              | Link experienced a loss of IMA frame (LIF) failure.                          |
| lods-failure             | Link experienced a loss of delay synchronization (LODS) failure.             |
| misconnected             | Link is misconnected to the far-end.                                         |
| blocked                  | Link is in blocked state.                                                    |
| fault                    | Link is in fault state.                                                      |
| far-end-tx-link-unusable | Far end Tx of the link is in an unusable state.                              |
| far-end-rx-link-unusable | Far end Rx of the link is in an unusable state.                              |

**Example** near-end-rx-failure-status = no-failure

**Location** DS1-ATM-STAT:ima-link-status

## near-end-rx-link-state

**Description** Indicates the near end receive (Rx) state of the link.

**Usage** Valid values for this read-only parameter are as follows:

| Value                    | Description                                     |
|--------------------------|-------------------------------------------------|
| not-in-group             | Link is not part of an IMA group.               |
| unusable-no-given-reason | Link is not usable but the reason is not known. |
| unusable-fault           | Link is not usable because of a fault.          |

| Value                 | Description                                                                    |
|-----------------------|--------------------------------------------------------------------------------|
| unusable-misconnected | Link is not usable because it is misconnected with the far end.                |
| unusable-inhibited    | Link is not usable because it is in an inhibited state.                        |
| unusable-failed       | Link is not usable because it is in failed state.                              |
| usable                | Link is usable.                                                                |
| active                | Link is active, part of an IMA group, and carrying traffic from the ATM layer. |

**Example** near-end-rx-link-state = not-in-group

**Location** DS1-ATM-STAT:ima-link-status

### near-end-rx-num-failures-counter

**Description** Read-only. Indicates the number of times a near-end receive failure alarm condition has been entered on this link.

Such conditions include loss of IMA frame (LIF), loss of delay synchronization (LODS), remote failure indication (RFI)-IMA, misconnection, and various forms of implementation-specific receive faults.

**Usage** The valid range for this read-only value is from (0) zero to 2147483647.

**Example** near-end-rx-num-failures-counter = 0

**Location** DS1-ATM-STAT:ima-link-statistic

### near-end-rx-unusable-secs-counter

**Description** Read-only. Indicates the number of received unusable seconds at the near-end receive (Rx) link.

**Usage** The valid range for this read-only value is from 0 to 4294967295 counts.

**Example** near-end-rx-unusable-secs-counter = 100

**Location** DS1-ATM-STAT:ima-link-statistic

## near-end-sev-errored-secs-counter

**Description** Read-only. Indicates the count of 1-second intervals during which 30 percent or more of the inverse multiplexing over ATM (IMA) Control Protocol (ICP) cells were counted as IV-IMA conditions or had one or more defects, except during unavailable seconds IMA (UAS-IMA) conditions. The count is for the current 15-minute interval.

Defects include link defects such as loss of synchronization (LOS), out of frame (OOF) or loss of frame (LOF) errors, Alarm Indication signals (AISs), or loss of cell delineation (LCD); loss of IMA frame (LIM) defects; or loss of delay synchronization (LODS) defects.

**Usage** The valid range for this read-only value is from 0 (zero) through 2147483647.

**Example** near-end-sev-errored-secs-counter = 0

**Location** DS1-ATM-STAT:ima-link-statistic

## near-end-tx-link-state

**Description** Read-only. Indicates the near end transmission state of the link.

**Usage** Valid values for this read-only parameter are as follows:

| Value                    | Description                                                                    |
|--------------------------|--------------------------------------------------------------------------------|
| not-in-group             | Link is not part of an IMA group.                                              |
| unusable-no-given-reason | Link is not usable but the reason is not known.                                |
| unusable-fault           | Link is not usable because of a fault.                                         |
| unusable-misconnected    | Link is not usable because it is misconnected with the far end.                |
| unusable-inhibited       | Link is not usable because it is in an inhibited state.                        |
| unusable-failed          | Link is not usable because it is in failed state.                              |
| usable                   | Link is usable.                                                                |
| active                   | Link is active, part of an IMA group, and carrying traffic from the ATM layer. |

**Example** near-end-tx-link-state = not-in-group

**Location** DS1-ATM-STAT:ima-link-status

## near-end-tx-num-failures-counter

**Description** Read-only. Indicates the number of times a near-end transmit failure alarm condition (some form of implementation-specific transmit fault) has been entered on this link.

**Usage** The valid range for this read-only value is from zero to 2147483647.

**Example** near-end-tx-num-failures-counter = 0

**Location** DS1-ATM-STAT:ima-link-statistic

## near-end-tx-unusable-secs-counter

**Description** Read-only. Indicates the number of transmitted unusable seconds at the near-end transmit (Tx) link.

**Usage** The valid range for this read-only value is from 0 to 4294967295 counts.

**Example** near-end-tx-unusable-secs-counter = 100

**Location** DS1-ATM-STAT:ima-link-statistic

## near-end-unavail-secs-counter

**Description** Read-only. Indicates the count of unavailable seconds at the near-end. Unavailability begins at the onset of 10 contiguous severely-errored-seconds inverse multiplexing over ATM (IMA) (SES-IMA) conditions and ends at the onset of 10 contiguous seconds with no severely errored IMA seconds.

**Usage** The valid range for this read-only value is from zero (0) to 2147483647.

**Example** near-end-unavail-secs-counter = 0

**Location** DS1-ATM-STAT:ima-link-statistic

## need-max-vpswitching-vpis

**Description** Increase the maximum number of VPCs on a slot by 3.

**Usage** Valid values are as follows:

- yes—Increase the maximum number of VPCs on a slot by 3.
- no (the default)—Do not increase the maximum number of VPCs on a slot.

**Example** set need-max-vpswitching-vpis = yes

**Dependencies** The use-vp-switching-workaround parameter must be set to yes for a yes setting in this parameter to have an effect.

**Location** SLOT-STATIC-CONFIG

**See Also** use-vp-switching-workaround

## neighbor-ip-address

**Description** Specifies the address of a Private Network-to-Network Interface (PNNI) neighbor reachable across this interface, to which a network management station can communicate.

**Usage** Specify an address in dotted decimal notation. The default is the null address 0.0.0.0.

**Example** `set neighbor-ip-address = 0.0.0.0`

**Location** ATM-IF-CONFIG:base-config

## neighbor-name

**Description** Specifies the textual name of the interface on the neighbor system.

**Usage** Specify a plain text string to designate the name. If the neighbor's interface does not have a name, this setting must be null (the default).

**Example** `set neighbor-name = r2d2`

**Location** ATM-IF-CONFIG:base-config

## neighbor-router-id

**Description** Specifies the router ID of the other end-point router in an Open Shortest Path First (OSPF) virtual link.

**Usage** Specify the IP address of an area border router, in dotted decimal notation.

**Example** `set neighbor-router-id =`

**Dependencies** The routers that make up a virtual link must have interfaces in a common nonbackbone area (the transit area), which cannot be a stub area.

**Location** OSPF-VIRTUAL-LINK

## netbios-primary-ns

**Description** Specifies the IP address of a primary NetBIOS server.

**Usage** Specify an IP address in dotted decimal notation.

**Example** `set netbios-primary-ns = 2.2.2.2/28`

**Location** IP-GLOBAL

## netbios-secondary-ns

**Description** Specifies the IP address of a secondary NetBIOS server. The Stinger unit accesses the secondary server if the primary NetBIOS server is unavailable.

**Usage** Specify an IP address in dotted decimal notation.

**Example** set netbios-secondary-ns = 2.2.2.2/28

**Location** IP-GLOBAL

## netmask

**Description** Specifies a subnet mask for the destination IP address of a private route. The value of netmask is set automatically when you specify a prefix length as part of the IP address.

**Usage** Specify a subnet mask in dotted decimal notation. The default is 0.0.0.0.

**Example** set netmask = 255.255.255.255

**Location** IP-INTERFACE

IP-ROUTE

PRIVATE-ROUTE-TABLE

## netmask-local

**Description** Specifies the netmask of the local interface address.

**Usage** Specify a netmask in IP address format. The default is 0.0.0.0.

**Example** set netmask-local = 255.255.255.0

**Location** CONNECTION:ip-options

CONNECTION:bir-options:multiple-ip-address:ip-address-option[n]

## netmask-remote

**Description** Specifies the netmask of the remote address.

**Usage** Specify a netmask in IP address format. The default is 0.0.0.0.

**Example** set netmask-remote = 255.255.255.0

**Location** CONNECTION:ip-options

CONNECTION:bir-options:multiple-ip-address:ip-address-option[n]

## network-loopback

**Description** Read-only. Indicates whether there is a line looped back out to the network.

**Usage** For this read-only parameter valid values are as follows:

- true—Indicates that a line is looped back to the network.
- false—Indicates that no line is looped back to the network.

**Example** network-loopback = false

**Location** DS1-ATM-STAT

T1-STAT

## network-management-enabled

**Description** Read-only. Indicates whether the network-management option is enabled.

**Usage** The network-management-enabled parameter is read-only. Valid values are as follows:

- yes—Indicates that the network-management option is enabled.
- no—Indicates that the network-management option is disabled.

**Example** network-management-enabled = yes

**Location** BASE

## network-mgmt-voip-enabled

**Description** Read-only. Indicates the status of network management for the Voice over IP (VoIP) feature.

**Usage** Read-only parameter with the following possible values:

- no—Network management VoIP feature is not enabled.
- yes—Network management VoIP feature is enabled.

**Example** network-mgmt-voip-enabled = yes

**Location** BASE

## network-type

**Description** Specifies or indicates a network type, as follows:

- In HDLSL2-STAT:physical-status and SHDSL-STAT:physical-status profiles, indicates the standard network type for an SHDSL line.
- In CONNECTION:ip-options:ospf-options and IP-INTERFACE:ospf profiles, specifies the type of network to which the interface connects.

**Usage** Valid values are as follows:

- In HDLSL2-STAT:physical-status and SHDSL-STAT:physical-status profiles, a read-only parameter with the following possible values:
  - annex-a
  - annex-b
  - annex-b-anfp
- In CONNECTION:ip-options:ospf-options and IP-INTERFACE:ospf profiles, specify one of the following values:
  - broadcast—Specifies any broadcast-capable network, such as Ethernet. (This is the default value in IP-INTERFACE/{ { any-shelf any-slot 0 } 0 }:ospf.)
  - nonbroadcast—Specifies an Open Shortest Path First (OSPF) nonbroadcast multiaccess (NBMA) network. An NBMA network has multiple points of access (more than two routers) and does not support broadcast capability. Frame relay and X.25 are typically NBMA networks.

- point-to-point—Specifies an interface connected to one other node on the remote end. (This is the default value in CONNECTION:ip-options:ospf-options.)

**Dependencies** Enabling the non-multicast parameter in the ospf-options subprofile causes the translation of the multicast traffic to directed traffic. This value is typically used with a serial link, such as a point-to-point connection over frame relay, and is not intended for use with NBMA configurations.

**Example** network-type = annex-b

**Location** CONNECTION:ip-options:ospf-options  
 HDLSL2-STAT:physical-status  
 IP-INTERFACE:ospf  
 SHDSL-STAT:physical-status

### ne-tx-clk-mode

**Description** Specifies the mode of the inverse multiplexing over ATM (IMA) group clocking.

**Usage** Valid values are as follows:

- ctc (the default)—Common transmit clock. Transmits clocks of the links within the IMA group are derived from the same clock source.
- itc—Independent transmit clock. Transmits clock of the links within the IMA group are derived from their respective receive clocks, as, for example, when group-symmetry-mode is set to symmetric-operation.

**Example** set ne-tx-clk-mode = ctc

**Location** IMAGROUP

### ne-tx-lid

**Description** Specifies the transmit LID for the link.

**Usage** Specify a number from (0) zero to 31.

**Example** set ne-tx-lid = 22

**Location** DS1-ATM:line-config:ima-option-config:txlink-config

### new-nas-port-id-format

**Description** Specifies whether to use the new network access server (NAS) port ID format.

**Usage** Valid values are as follows:

- yes—Specifies that the new NAS port ID format is used. This is the default.
- no—Specifies that the old NAS port ID is used.



**Example** `set new-nas-port-id-format = yes`

**Location** `SYSTEM`

### `nm-copper-loop-test-enabled`

**Description** Read-only. Indicates the status of the copper loop test feature.

**Usage** Read-only parameter with the following possible values:

- `yes`—Copper loop test feature is enabled.
- `no` (the default)—Copper loop test feature is not enabled.

**Example** `nm-copper-loop-test-enabled= yes`

**Location** `BASE`

### `nm-navis-radius-enabled`

**Description** Read-only. Indicates the status of the NavisRadius™ feature.

**Usage** Read-only parameter with the following possible values:

- `yes`—NavisRadius™ feature is enabled.
- `no` (the default)—NavisRadius™ feature is not enabled.

**Example** `nm-navis-radius-enabled = yes`

**Location** `BASE`

### `nm-prov`

**Description** Read-only. Indicates the status of the Navis™ Provisioning Server for edge devices support feature.

**Usage** Read-only parameter with the following possible values:

- `yes`—Navis™ Provisioning Server for edge devices support feature is enabled.
- `no` (the default)—Navis™ Provisioning Server for edge devices support feature is not enabled.

**Example** `nm-prov = yes`

**Location** `BASE`

**nm-prov-core**

**Description** Read-only. Indicates the status of Navis™ Provisioning Server support for edge and core devices feature.

**Usage** Read-only parameter with the following possible values:

- **yes**—Navis™ Provisioning Server support for edge and core devices feature is enabled.
- **no** (the default)—Navis™ Provisioning Server support for edge and core devices feature is not enabled.

**Example** nm-prov-core = yes

**Location** BASE

**nm-reporting-enabled**

**Description** Read-only. Indicates the status of the reporting feature.

**Usage** Read-only parameter with the following possible values:

- **yes**—Reporting feature is enabled.
- **no** (the default)—Reporting feature is not enabled.

**Example** nm-reporting-enabled = yes

**Location** BASE

**nm-vpn-enabled**

**Description** Read-only. Indicates the status of the virtual private network (VPN) feature.

**Usage** Read-only parameter with the following possible values:

- **yes**—VPN feature is enabled.
- **no** (the default)—VPN feature is not enabled.

**Example** nm-vpn-enabled = yes

**Location** BASE

## noattr6-use-termsrv

**Description** Specifies whether the unit initiates a terminal-server login if it does not receive a RADIUS Service-Type (6) attribute.

**Usage** Valid values are as follows:

- **yes**—Specifies that the Stinger unit initiates a terminal-server login if Service-Type is not received, regardless of whether Framed-Protocol (7) is received or not. This is the default.
- **no**—Specifies the following:
  - If Service-Type is not received, but Framed-Protocol is received, a framed-protocol login is initiated.
  - If neither Service-Type nor Framed-Protocol is received, a terminal-server login is initiated.

**Example** `set noattr6-use-termsrv = no`

**Location** EXTERNAL-AUTH

## node-admin-status

**Description** Specifies the administrative status of a Private Network-to-Network Interface (PNNI) node.

**Usage** Valid values are as follows:

- **up** (the default)—Specifies that the node is allowed to become active.
- **down**—Specifies that the node is forced to become inactive.

**Example** `set node-admin-status = up`

**Location** PNNI-NODE-CONFIG

## node-atm-address

**Description** Specifies the network service access point (NSAP) ATM address that identifies the Stinger unit as a node within a Private Network-to-Network Interface (PNNI) network.

**Usage** Remote systems that exchange PNNI protocol packets with the node direct packets or calls to this address.

**Example** `set node-atm-address =  
39:84:0f:80:01:bc:72:00:01:d0:6a:96:00:ff:d0:6a:96+`

**Location** PNNI-NODE-CONFIG

## node-complex-rep

**Description** Enables or disables complex node representation in Private Network-to-Network Interface (PNNI) network. Complex representation provides information omitted in simple representation, but slows transmission.

**Usage** Valid values are as follows:

- `true`—Complex node representation is used.
- `false` (the default)—Simple node representation is used.

**Example** `set node-complex-rep = true`

**Location** PNNI-NODE-CONFIG

## node-domain-name

**Description** Specifies the name of the Private Network-to-Network Interface (PNNI) routing domain.

**Usage** All lowest-level PNNI nodes with the same domain name are presumed to be connected.

**Example** set node-domain-name = segundo

**Location** PNNI-NODE-CONFIG

## node-id

**Description** Specifies a number that identifies a Private Network-to-Network Interface (PNNI) node within a peer group.

**Usage** If both this parameter and the `node-peer-group-id` parameter have the default value of zero, the system derives the PNNI node ID from the node ATM address and other values.

Or you can manually specify a 22-byte, 44-digit hexadecimal number as a node ID.

**Example** set node-id = 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00+

**Location** PNNI-NODE-CONFIG

## node-index

**Description** Specifies the Private Network-to-Network Interface (PNNI) node index.

**Usage** Only node index 1 is currently supported.

**Example** set node-index = 1

```
Location PNNI-METRICS:metrics-index
PNNI-NODE-CONFIG
PNNI-ROUTE-TNS
PNNI-SUMMARY-ADDR:addr-index
```

## node-level

**Description** Specifies the Private Network-to-Network Interface (PNNI) routing-level indicator.

**Usage** Specify a number from 0 to 104, representing the level of the PNNI hierarchy at which this node exists.

**Example** `set node-level = 96`

**Location** PNNI-NODE-CONFIG

## node-lowest

**Description** Enables or disables lowest-level node status for a Private Network-to-Network Interface (PNNI) node.

**Usage** Valid values are as follows:

- `true` (the default)—Specifies that the node is a lowest-level node.
- `false`—*The false setting is not currently supported.*

**Example** `set node-lowest = true`

**Location** PNNI-NODE-CONFIG

## node-peer-group-id

**Description** Specifies a number used to group nodes into a Private Network-to-Network Interface (PNNI) peer group.

**Usage** All members of the same PNNI peer group have the same peer group ID. If both this parameter and the `node-id` parameter have the default value of zero, the system derives the PNNI peer group ID from the Asynchronous Transfer Mode (ATM) node address and other values.

Or you can manually specify a 14-byte, 28-digit hexadecimal number as a peer group ID.

**Example** `set node-peer-group-id = 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00`

**Location** PNNI-NODE-CONFIG

## node-restricted-transit

**Description** Specifies whether to enable or disable support of switched virtual channels (SVCs) transiting the node.

**Usage** Valid values are as follows:

- `true`—The node prevents the transit of SVCs.
- `false` (the default)—The node allows transit of SVCs.

**Example** `set node-restricted-transit = false`

**Location** `PNMI-NODE-CONFIG`

## `noise-margin-down`

**Description** Read-only. Indicates the current downstream noise margin of the asymmetric digital subscriber line (ADSL) in decibels (dB).

**Usage** The noise-margin-down value is read-only.

**Example** `noise-margin-down = 6`

**Location** `AL-DMT-STAT:physical-statistic`

## `noise-margin-up`

**Description** Read-only. Indicates the current upstream noise margin of the asymmetric digital subscriber line (ADSL) in decibels (dB).

**Usage** The noise-margin-up value is read-only.

**Example** `noise-margin-up = 6`

**Location** `AL-DMT-STAT:physical-statistic`

## `non-multicast`

**Description** Specifies whether all multicast packets are remapped to a directed neighbor address.

**Usage** Valid values are as follows:

- `yes`—Specifies that all multicast packets are remapped to a directed neighbor address, enabling adjacencies to form between neighbors. This setting is ignored on Ethernet (a broadcast network). Its use is not recommended for unnumbered interfaces. If you specify it for a nonnumbered interface, the Stinger unit drops the packets.
- `no` (the default)—Specifies that multicast packets are not remapped to a directed neighbor address.

**Example** `set non-multicast = yes`

**Location** `CONNECTION:ip-options:ospf-options`  
`IP-INTERFACE:ospf`

## non-real-time-vbr

**Description** Enables and disables variable bit rate (VBR)-nonreal time traffic in the queue containing this parameter.

**Usage** Valid values are as follows:

- yes—This queue supports ATM VBR-nonreal time traffic.
- no—The queue does not support VBR-nonreal time traffic. This is the default.

**Example** `set non-real-time-vbr = no`

**Dependencies** For each queue, one or more ATM services categories can be set to yes. The `non-real-time-vbr` parameter must be set to yes for at least one and no more than two of the active queues assigned to a line interface module (LIM), control module, or trunk module.

**Location** `SWITCH-CONFIG:atm-parameters:outgoing-queue`

## notification-log-age-out

**Description** Specifies the number of minutes that an SNMP trap (notification) is kept in a log before it is automatically removed.

**Usage** Specify a number from 0 to 2147483647. The default is 1440 (24 hours). If you specify 0 (zero), a notification is kept in a log indefinitely.

**Example** `set notification-log-age-out = 2880`

**Location** `SNMP`

## notification-log-enable

**Description** Specifies whether SNMP traps (notifications) for this profile are to be logged.

**Usage** Valid values are as follows:

- yes—Enables logging.
- no (the default)—Disables logging.

**Example** `set notification-log-enable = yes`

**Location** `TRAP`

## notification-log-limit

**Description** Specifies the maximum number of trap (notification) entries that can be held in the SNMP notification log.

**Usage** Specify a number from 1 to 500. The default is 50.

**Example** `set notification-log-limit = 100`

**Location** `TRAP`

## notify-tag-list

**Description** Specifies the tag list that is specified by the `tag` parameter value in each occurrence of the `snmpv3-notification` profile.

**Usage** Specify the tag value(s) you specified in one or more `snmpv3-notification` profiles.

**Example** `set notify-tag-list = default1`

**Location** TRAP

## notify-view-name

**Description** Specifies the name of a view for notify access in a view-based access control model (VACM).

**Usage** Specify a name of up to 32 characters. If a request that matches the access properties specified in this profile uses this name, read access is granted.

**Example** `set notify-view-name = notify1`

**Location** VACM-ACCESS

## no-trunk-alarm

**Description** Enables or disables setting an alarm relay when no trunk is available.

**Usage** Valid values are as follows:

- `no` (the default)—Does not set an alarm relay when no trunk is available.
- `yes`—Sets an alarm relay when no trunk is available.

**Example** `set no-trunk-alarm = yes`

**Location** SYSTEM

## np-default-filtering-policy

**Description** Specifies the default filtering policy to be used at the input side of the interface during the `np-update-time` interval, before the batched hardware update has been done.

**Usage** The following are valid values:

- `drop`—The `drop` policy has an impact on random access memory size, because the system must create a forwarding rule for non-filtered connections.
- `forward`—If `np-update-time` is set to zero, it is strongly recommended to use the `forward` policy. This is the default value.



**Example** `set np-default-filtering-policy = drop`

**Dependencies** A system reset is required for a new value of this parameter to take effect.

**Location** `SYSTEM`

## `np-update-time`

**Description** Interval (in seconds) at which to communicate filtering or flow classification updates to the underlying hardware.

**Usage** Valid values are from 0 to 20. The default value is 0.

**Example** `set np-update-time = 10`

**Location** `SYSTEM`

## `ntr-enabled`

**Description** Enables or disables network time reference (NTR) functionality.

**Usage** Valid values are as follows:

- `no`—Disables NTR functionality. This is the default.
- `yes`—Enables NTR functionality.

**Example** `set ntr-enabled = yes`

**Dependencies** If `unit-type` is `coe` (central office equipment), the system clock signal is used as the input and the customer premises equipment (CPE), if equipped to do so, can recover the clock.

If `unit-type` is `cpe`, the port outputs the recovered clock signal as the system clock if `clock-source` is set to `eligible` and `clock-priority` is set so that the clock can be selected.

**Location** `HDLSL2:line-config`  
`SHDSL:line-config`

## `number-of-channels`

**Description** Read-only. Indicates the number of channels in this protection group.

**Usage** The valid range for this read-only parameter is from 0 through 255.

**Example** `number-of-channels = 2`

**Location** `APS-STAT`

## num-digits-trunk-groups

**Description** Specifies the number of digits to allow for trunk groups.

**Usage** Specify a number from 1 to 4:

- When you accept the default of 1, trunk-group numbers range from 2 to 9, and the dial-out telephone number is preceded by a single-digit number.
- If num-digits-trunk-groups is set to 2, 3, or 4, the range of trunk-group numbers can include the specified number of digits (up to 9999), and the dial-out telephone number is always preceded by that number of digits.

For example, if you set num-digits-trunk-groups to 2, and you want the device to dial the number 555-1212 on trunk 7, the dial-out telephone string is 075551212.

**Example** set num-digits-trunk-groups = 2

**Dependencies** Consider the following:

- When the Stinger unit is configured to interoperate with an external application for dial-out, the external system and the Stinger unit must agree about the number of digits in a trunk-group number. Otherwise, telephone numbers are not parsed correctly and calls fail.
- use-trunk-groups must be set to yes for num-digits-trunk-groups to have an effect.

**Location** SYSTEM

## num-of-vci

**Description** Maximum number of VCIs that can be allocated on the module in this slot.

**Usage** Valid values are as follows:

- one-k—indicates that 1024 VCIs can be allocated by the card.
- two-k (the default)—indicates that 2048 VCIs are available for allocation.

**Example** set num-of-vci = one-k

**Dependencies** On a fully loaded system, reducing the number of VCIs on at least six LIM slots is recommended.

This parameter applies only to the LIM slots of a standalone or host Stinger system. A system reset is required to recognize the new value.

Changing the default setting for this parameter is not recommended for OLIMs on a fully loaded Stinger system.

## num-sec-invalid

**Description** Read-only. Indicates how many error seconds were detected during the continuous bit error-rate test (BERT).

**Usage** The num-sec-invalid value is read-only.

**Location** AL-DMT-STAT:physical-status

## num-sec-valid

**Description** Read-only. Indicates how many seconds were error-free during the continuous bit error-rate test (BERT).

**Usage** The num-sec-valid value is read-only.

**Location** AL-DMT-STAT:physical-status

## nvr-am-was-rebuilt

**Description** Read-only. Indicate nonvolatile RAM (NVRAM) rebuild status.

**Usage** Read-only parameter with one of the following values:

- no—NVRAM was not rebuilt.
- yes—NVRAM was rebuilt.

**Example** nvr-am-was-rebuilt = yes

**Location** SYSTEM

## O

### oam-address

**Description** Specifies information about the ATM interface on which a test is carried out.

**Usage** Specify shelf, slot, port, vpi, and vci values. The shelf number is always 1 (one).

- When you specify 0 (zero) for the port value, the tests are performed on all ports on the specified slot.
- When you specify 32768 for the vpi value, the tests are performed for all virtual path identifiers (VPIs) on the specified slot and port.
- When you specify 32768 for the vci value, the tests are performed for all virtual channel identifiers (VCIs) on the specified slot and port.
- When you specify 32769 for the vci value, an F4 test is performed. For F5 testing, you must specify a vci value greater than 31.

**Example** The following example specifies that a test is to be performed on the ATM interface port 5 in slot 3, with VPI 4, and VCI 5:

```
admin> set oam-address = {{1 3 5}4 2}
admin> list oam-address

[in ATM-OAM/{ { shelf-1 slot-3 5 } 4 2 }:oam-address (new) (changed)]
physical-address = { shelf-1 slot-3 5 }
vpi = 4
vci = 2
```

**Location** OAM-ADDRESS

### oam-ais-f5

**Description** oam-ais-f5 is not supported with the current software version.

**Location** CONNECTION:atm-options  
CONNECTION:atm-connect-options

### oam-support

**Description** Enables or disables F4 or F5 operations, administration, and maintenance (OAM) support on a virtual path connection (VPC).

**Usage** Valid values are as follows:

- yes (the default)
- no

**Example** set oam-support = yes

#### Dependencies

- Set the oam-support parameter to yes and the vp-switching parameter to yes to enable F4 OAM support on the VPC.
- Set the oam-support parameter to no and the vp-switching parameter to yes to disable F4 OAM support on the VPC.
- Set the oam-support parameter to yes and the vp-switching parameter to no to enable F4 and F5 OAM support and end-to-end functionalities on the VPC.
- Set the oam-support parameter to no and the vp-switching parameter to no to disable F5 OAM support and enable F4 OAM support and end-to-end functionalities on the VPC.

**Location** CONNECTION:atm-connect-options  
CONNECTION:atm-options

### oam-timeout-trap-enabled

**Description** Enables or disables an operations, administration, and maintenance (OAM) trap.

**Usage** Valid values are as follows:

- yes—Enables the OAM trap.
- no (the default)—Disables the OAM trap.

**Example** set oam-timeout-trap-enabled = yes

**Location** TRAP

### offset

**Description** Specifies a byte offset from the start of a packet to the start of the data in the packet to be tested in the generic filter. The packet data is compared to the value setting specified in the filter.

If the current filter is linked to the previous one (if more is set to yes in the previous filter), the offset starts at the end point of the previous segment.

**Usage** Specify a number from 0 to 8. The default is 0 (zero), which indicates no offset.

**Example** set offset = 2

**Dependencies** This setting applies only if the type parameter in the input-filter or output-filter subprofile is set to generic-filter.

**Location** FILTER:input-filters[n]:gen-filter  
FILTER:output-filters[n]:gen-filter

### oif-anomalies-counter

**Description** Indicates the number of out-of-IMA-frame (OIF) anomalies in inverse multiplexing over ATM (IMA), except during severely-errored-seconds IMA (SES-IMA) or unavailable seconds IMA (UAS-IMA) conditions, in the current 15-minute interval.

**Usage** The valid range for this read-only value is from 0 (zero) to 2147483647.

**Example** `oif-anomalies-counter = 213`

**Location** `DS1-ATM-STAT:ima-link-statistic`

### old-call-filter

**Description** Specifies the number of the filter used to determine if a packet should cause the idle timer to be reset.

**Usage** Specify a numeric value in a range of 0 (zero) to 32. The default is 0.

**Example** `set old-call-filter = 4`

**Location** `CONNECTION:session-options`

### old-data-filter

**Description** Specifies the number of the filter used to determine if packets should be forwarded or dropped.

**Usage** Specify a numeric value in a range of 0 (zero) to 32. The default is 0.

**Example** `set old-data-filter = 4`

**Location** `CONNECTION:session-options`

### only-one-correction

**Description** Enables or disables use of only one instead of many switching fabric corrections.

**Usage** Valid values are as follows:

- `yes` (the default)—Switching fabric corrections can occur only once. One correction is recommended.
- `no`—Switching fabric corrections can occur many times.

**Example** `set only-one-correction = no`

**Location** `SYSTEM-INTEGRITY:integrity-config`

## operational-count

**Description** Read-only. Indicates the number of devices that are in the UP state.

**Usage** The operational-count setting is read-only.

**Example** operational-count = 10

**Location** DEVICE-SUMMARY

## operational-mode

**Description** Read-only. Indicates the mode in which the modem operates as automatically detected or as set by user.

**Usage** Valid values for this read-only parameter are as follows:

- ansi-dmt
- g-lite
- g-dmt
- unknown

**Example** operational-mode = g-lite

**Location** AL-DMT-STAT:physical-status

## operational-rate

**Description** Read-only. Indicates the data rate for the symmetrical interface to which this parameter applies.

**Usage** The data rate is currently fixed at 1.544Mbps.

**Example** operational-rate = 1544000

**Location** HDLSL2-STAT:physical-status  
SHDSL-STAT:physical-status

## oper-status

**Description** Read-only. Indicates the operational status of the reachable address and whether it is being advertised by this Private Network-to-Network Interface (PNNI) node.

**Usage** Valid values for this read-only parameter are as follows:

- inactive—The prefix is not reachable.
- active—The prefix is reachable and is not being advertised in PNNI.
- advertised—The prefix is reachable and is being advertised in PNNI.

**Example** oper-status = inactive

**Location** PNNI-ROUTE-ADDR

## organization-minus-1

**Description** *Not used.* Specifies a number representing the highest level of the Private Network-to-Network Interface (PNNI) hierarchy that lies within the organization-minus-one scope.

**Usage** Specify a number from 0 to 104. The default value is 72.

**Location** PNNI-NODE-CONFIG:node-scope-mapping

## organization-plus-1

**Description** *Not used.* Specifies the highest level of the Private Network-to-Network Interface (PNNI) hierarchy that lies within the organization-plus-one scope.

**Usage** Specify a number from 0 to 104. The default value is 64.

**Location** PNNI-NODE-CONFIG:node-scope-mapping

## originate-advert

**Description** Specifies whether or not the reachable address is to be advertised by the local node into its Private Network-to-Network Interface (PNNI) routing domain.

**Usage** Valid values are as follows:

- `true` (the default)—The local node advertises reachability of the address into the routing domain.
- `false`—The local node does not advertise the reachable address.

**Example** `set originate-advert = true`

**Location** PNNI-ROUTE-ADDR

## ospf-approaching-overflow-enabled

**Description** Enables or disables trap (notification) generation if the number of link state advertisements (LSAs) in the router's link-state database has exceeded 90 percent of OSPFExtLsdbLimit (OSPF trap 15).

**Usage** Specify one of the following settings:

- `yes`—Enables generation of OSPF trap 15.
- `no` (the default)—Disables generation of OSPF trap 15.

**Example** `set ospf-approaching-overflow-enabled = yes`

**Location** TRAP



## ospf-ase-pref

**Description** Specifies the preference value for Open Shortest Path First (OSPF) routes that the router learns about by means of Routing Information Protocol (RIP), Internet Control Message Protocol (ICMP), or another non-OSPF protocol.

When choosing the routes to put in the routing table, the router first compares their preference values, preferring the lowest number. If the preference values are equal, the router compares the metric values, using the route with the lowest metric.

**Usage** Specify a number from 0 through 255. A value of 255 prevents the use of the route. Following are the default preferences for different types of routes:

- 0 (zero)—Connected routes
- 10—OSPF routes
- 30—Routes learned from ICMP redirects
- 100—Routes learned from RIP
- 100—Static routes

**Example** `set ospf-ase-pref = 100`

**Location** IP-GLOBAL

## ospf-enabled

**Description** Enables or disables generation of Open Shortest Path First (OSPF) traps (notifications) to signal the occurrence of any of the following events:

- `OspfIfConfigError`
- `OspfIfAuthFailure`
- `OspfIfStateChange`
- `OspfIfRxBadPacket`
- `OspfTxRetransmit`
- `OspfNbrStateChange`
- `OspfVirtIfStateChange`
- `OspfVirtIfRxBadPacket`
- `OspfVirtIfTxRetransmit`
- `OspfVirtNbrStateChange`
- `OspfOriginateLsa`
- `OspfMaxAgeLsa`
- `OspfLsdbOverflow`
- `OspfLsdbApproachingOverflow`

**Usage** Valid values are as follows:

- `yes`—Specifies that trap generation depends on whether the specific OSPF trap is enabled.
- `no` (the default)—Specifies that OSPF traps are generated regardless of individual OSPF trap settings in the profile.

**Example** ospf-enabled = yes

**Location** TRAP

## ospf-if-config-error-enabled

**Description** Enables or disables trap (notification) generation if a packet has been received on a nonvirtual interface from a router whose configuration conflicts with this router's configuration (OSPF trap 4).

**Usage** Valid values are as follows:

- yes—Specifies that OSPF trap 4 is generated if a packet has been received on a nonvirtual interface from a router whose configuration conflicts with this router's configuration.
- no (the default)—Specifies that OSPF trap 4 is not generated if a packet has been received on a nonvirtual interface from a router whose configuration conflicts with this router's configuration.

**Example** set ospf-if-config-error-enabled = yes

**Dependencies** The event `optionMismatch` causes a trap only if it prevents an adjacency from forming.

**Location** TRAP

## ospf-if-rx-bad-packet

**Description** Enables or disables trap (notification) generation if an Open Shortest Path First (OSPF) packet has been received on a nonvirtual interface that cannot be parsed (OSPF trap 8).

**Usage** Valid values are as follows:

- yes—Specifies that OSPF trap 8 is generated if an OSPF packet has been received on a nonvirtual interface that cannot be parsed.
- no (the default)—Specifies that OSPF trap 8 is not generated if an OSPF packet has been received on a nonvirtual interface that cannot be parsed.

**Example** set ospf-if-rx-bad-packet = yes

**Location** TRAP

## ospf-if-state-change-enabled

**Description** Enables or disables trap (notification) generation if the state of a nonvirtual Open Shortest Path First (OSPF) interface has changed (OSPF trap 16). This trap is generated when the interface state regresses (for example, goes from Dr to Down) or progresses to a terminal state (Point-to-Point, DR Other, Dr, or Backup).

**Usage** Valid values are as follows:

- **yes**—Specifies that OSPF trap 16 is generated if the state of a nonvirtual OSPF interface has changed.
- **no** (the default)—Specifies that OSPF trap 16 is not generated if the state of a nonvirtual OSPF interface has changed.

**Example** `set ospf-if-state-change-enabled = yes`

**Location** TRAP

## ospf-lsdb-overflow-enabled

**Description** Enables or disables trap (notification) generation if the number of link state advertisements (LSAs) in the router's link-state database has exceeded `OSPFExtLsdbLimit` (OSPF trap 14).

**Usage** Valid values are as follows:

- **yes**—Specifies that OSPF trap 14 is generated if the number of LSAs in the router's link-state database has exceeded `OSPFExtLsdbLimit`.
- **no** (the default)—Specifies that OSPF trap 14 is not generated if the number of LSAs in the router's link-state database has exceeded `OSPFExtLsdbLimit`.

**Example** `ospf-lsdb-overflow-enabled = yes`

**Location** TRAP

## ospf-maxagelsa-enabled

**Description** Enables or disables trap (notification) generation if a link state advertisement (LSA) in the router's link-state database has aged to `MaxAge` (OSPF trap 13).

**Usage** Specify one of the following settings:

- **yes**—Specifies that OSPF trap 13 is generated if an LSA in the router's link-state database has aged to `MaxAge`.
- **no** (the default)—Specifies that OSPF trap 13 is not generated if an LSA in the router's link-state database has aged to `MaxAge`.

**Example** `ospf-maxagelsa-enabled = yes`

**Location** TRAP

**ospf-max-lsa**

**Description** Specifies the maximum number of link state advertisements (LSAs) allowed in the link-state database.

**Usage** Specify a number from 0 through 4294967295. The default setting is 0.

**Example** `set ospf-max-lsa = 10`

**Location** IP-GLOBAL

**ospf-nbr-state-change-enabled**

**Description** Enables or disables trap (notification) generation if the state of a nonvirtual Open Shortest Path First (OSPF) neighbor has changed (OSPF trap 2).

**Usage** Valid values are as follows:

- **yes**—Specifies that OSPF trap 2 is generated if the state of a nonvirtual OSPF neighbor has changed.
- **no** (the default)—Specifies that OSPF trap 2 is not generated if the state of a nonvirtual OSPF neighbor has changed.

**Example** `ospf-nbr-state-change-enabled = yes`

**Dependencies** OSPF trap 2 is generated when the neighbor state regresses (for example, changes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (for example, 2-Way or Full). When a neighbor transitions from or to Full on nonbroadcast multiaccess (NBMA) and broadcast networks, the trap is generated by the designated router. A designated router transitioning to Down is noted by OSPFIIfStateChange.

**Location** TRAP

**ospf-originatelsa-enabled**

**Description** Enables or disables trap (notification) generation if a new link state advertisement (LSA) has been originated by this router due to a topology change (OSPF trap 12).

**Usage** Valid values are as follows:

- **yes**—Specifies that the unit generates OSPF trap 12 if a new LSA has been originated by this router due to a topology change.
- **no** (the default)—Specifies that the unit does not generate OSPF trap 12 if a new LSA has been originated by this router due to a topology change.

**Example** `set ospf-originatelsa-enabled = yes`

**Location** TRAP

## ospf-pref

**Description** Specifies the preference for routes that the router learns about by means of the Open Shortest Path First (OSPF) protocol.

When choosing the routes to put in the routing table, the router first compares their preference values, preferring the lowest number. If the preference values are equal, the router compares the metric values, using the route with the lowest metric.

**Usage** Specify a number from 0 through 255. A value of 255 prevents the use of the route. Following are the default preferences for different types of routes:

- 0 (zero)—Connected routes
- 10—OSPF routes
- 30—Routes learned from Internet Control Message Protocol (ICMP) redirects
- 100—Routes learned from Routing Information Protocol (RIP)
- 100—Static routes
- 100—Ascend Tunnel Management Protocol (ATMP) routes

**Example** `set ospf-pref = 10`

**Location** IP-GLOBAL

## ospf-set-trap

**Description** Enables/disables open shortest path first (OSPF) traps. This parameter can be set using Simple Network Management Protocol (SNMP).

**Usage** Specify a hexadecimal value of 4 bytes.

**Example** `set ospf-set-trap = 00:00:00:00`

**Location** OSPF-GLOBAL

## ospf-tx-retransmit-enabled

**Description** Enables or disables trap (notification) generation if an Open Shortest Path First (OSPF) packet has been retransmitted on a nonvirtual interface (OSPF trap 10). All packets that are retransmitted are associated with a link-state database (LSDB) entry. The LS type, LS ID, and Router ID are used to identify the LSDB entry.

**Usage** Valid values are as follows:

- `yes`—Specifies that the unit generates OSPF trap 10 if an OSPF packet has been retransmitted on a nonvirtual interface.
- `no` (the default)—Specifies that the unit does not generate OSPF trap 10 if an OSPF packet has been retransmitted on a nonvirtual interface.

**Example** `set ospf-tx-retransmit-enabled = yes`

**Location** TRAP

### ospf-virt-if-rx-bad-packet

**Description** Enables or disables trap (notification) generation if an Open Shortest Path First (OSPF) packet has been received on a virtual interface that cannot be parsed (OSPF trap 9).

**Usage** Valid values are as follows:

- **yes**—Specifies that the unit generates OSPF trap 9 if an OSPF packet has been received on a virtual interface that cannot be parsed.
- **no** (the default)—Specifies that the unit does not generate OSPF trap 9 if an OSPF packet has been received on a virtual interface that cannot be parsed.

**Example** `set ospf-virt-if-rx-bad-packet = yes`

**Location** TRAP

### ospf-virt-if-state-change-enabled

**Description** Enables or disables trap (notification) generation if the state of an Open Shortest Path First (OSPF) virtual interface has changed (OSPF trap 1).

**Usage** Valid values are as follows:

- **yes**—Specifies that the unit generates OSPF trap 1 if the state of an OSPF virtual interface has changed.
- **no** (the default)—Specifies that the unit does not generate OSPF trap 1 if the state of an OSPF virtual interface has changed.

**Example** `set ospf-virt-if-state-change-enabled = yes`

**Location** TRAP

### ospf-virt-if-tx-retransmit-enabled

**Description** Enables or disables trap (notification) generation if an Open Shortest Path First (OSPF) packet has been retransmitted on a virtual interface (OSPF trap 11). All packets that are retransmitted are associated with a link-state database (LSDB) entry. The LS type, LS ID, and Router ID are used to identify the LSDB entry.

**Usage** Valid values are as follows:

- **yes**—Specifies that the unit generates OSPF trap 11 if an OSPF packet has been retransmitted on a virtual interface.
- **no** (the default)—Specifies that the unit does not generate OSPF trap 11 if an OSPF packet has been retransmitted on a virtual interface.

**Permission level** `set ospf-virt-if-tx-retransmit-enabled = yes`

**Location** TRAP

## ospf-virt-nbr-state-change-enabled

**Description** Enables or disables trap (notification) generation if the state of an Open Shortest Path First (OSPF) virtual neighbor has changed (OSPF trap 3).

**Usage** Valid values are as follows:

- **yes**—Specifies that the unit generates OSPF trap 3 if the state of an OSPF virtual neighbor has changed.
- **no** (the default)—Specifies that the unit does not generate OSPF trap 3 if the state of an OSPF virtual neighbor has changed.

**Example** `set ospf-virt-nbr-state-change-enabled = yes`

**Location** TRAP

## out-defect-int-time

**Description** Specifies the time, in milliseconds, that must elapse before the FAILED state condition can be turned off for the receiving link of an inverse multiplexing over ATM (IMA) connection.

If the NO DEFECT condition persists for this time, the link leaves the FAILED state.

**Usage** Valid values are from 0 (zero) to 2147483647. The default is 10000.

**Example** `set out-defect-int-time = 10000`

**Location** DS1-ATM:line-config:ima-option-config:rxlink-config

## outgoing-cells

**Description** Read-only. Indicates the number of outgoing cells in an asymmetric digital subscriber (ADSL) line.

**Usage** The outgoing-cells value is read-only.

**Example** `outgoing-cells = 100`

**Location** AL-DMT-STAT:physical-statistic

## out-of-cell-delineation

**Description** Read-only. Indicates whether the device is receiving a far-end loss-of-frame signal, also known as a *Yellow Alarm*.

**Usage** The out-of-cell-delineation value is read-only. Valid values are as follows:

- **true**—Indicates that the device is receiving a far-end loss-of-frame signal.
- **false**—Indicates that the device is not receiving a far-end loss-of-frame signal.

**Example** `out-of-cell-delineation = false`

**Location** OC3-ATM-STAT

## out-of-frame

**Description** Read-only. Indicates whether the local line is connected and in frame.

**Usage** Valid values are as follows:

- true —Indicates that near end is out of frame.
- false —Indicates that the line is connected and in frame.

**Example** out-of-frame = false

**Location** OC3-ATM-STAT

## output-power-down

**Description** Read-only. Indicates the current downstream aggregate power level in decibels (dB).

**Usage** The output-power-down value is read-only.

**Example** output-power-down = 19

**Location** AL-DMT-STAT:physical-statistic

## output-power-up

**Description** Read-only. Indicates the current upstream aggregate power level in decibels (dB).

**Usage** The output-power-up value is read-only.

**Example** output-power-up = 19

**Location** AL-DMT-STAT:physical-statistic

## override-delay

**Description** Specifies the number of seconds a Private Network-to-Network Interface (PNNI) node waits for itself to be declared the preferred peer group leader (PGL) by unanimous agreement among its peers.

When unanimous agreement is not reached, *override-delay* specifies the number of seconds that must pass before the node considers a two-thirds majority as sufficient agreement to declare itself peer group leader, abandoning the attempt to get unanimous agreement.

**Usage** Specify the number of seconds. The default is 30.

**Example** set override-delay = 50

**Location** PNNI-NODE-CONFIG:node-pgl



## override-interval

**Description** A delay interval, in milliseconds, used to randomize when scheduling a delayed join message.

**Usage** The valid range is from 1 to 65535 with a default value of 2500 milliseconds.

**Example** `set override-interval = 1000`

**Location** IP-INTERFACE:pim-options  
CONNECTION:ip-options:pim-options

## over-subscription

**Description** Specifies the allowed oversubscription to the line rate for connection admission control (CAC).

Oversubscription modifies the allowed bandwidth on a port. The allowed bandwidth on a trunk port is equal to line-rate multiplied by over-subscription divided by 10 (line-rate \* over-subscription/ 10).

**Usage** Valid values range from 0 (zero) to 10240. The default value is 10. Consider the following:

- The default value (10) limits the port to accept only connections that do not exceed line-rate.
- Values between 1 and 9 limit the allowed bandwidth to a value less than line-rate.
- A value of 0 (zero) disables the port from taking part in any CAC. The bandwidth is advertised as 0.

**Example** `set over-subscription = 50`

**Location** HIGH-SPEED-SLOT-STATIC-CONFIG:trunk-cac-config



**Note** This parameter was previously located in the atm-config profile. Its use in that location has been deprecated.

## over-temperature

**Description** Indicates whether the cabinet temperature exceeds the threshold.

**Usage** This parameter is read-only. Valid values are as follows:

- yes—The cabinet temperature exceeds the threshold.
- no (the default)—The cabinet temperature is within acceptable limits.

**Example** `over-temperature = no`

**Location** REMOTE-SHELF-STAT

## P

### pair

**Description** Read-only. Indicates identity and reboot statistics for the other controller in this context.

**Usage** Read-only, complex field.

**Example** `pair = { 9487770 }`

**Location** `REDUNDANCY-STATS:context-stats`

### parallel-dialing

**Description** Specifies the number of Call-Setup requests the system sends to the network side at any given time.

If the system is processing the maximum number of calls when it receives a new call request, it queues the request and processes it after the network side sends a call-proceeding message for a previous request.

**Usage** Specify an integer from 1 to 64. The default is 12. Consider the following:

- If the Stinger unit has trouble establishing an initial connection at the full bandwidth for calls from the U.S. to another country, reduce `parallel-dialing` to a value of 1.
- For ADSL or SDSL operation, you must set `parallel-dialing` to the number of ADSL or SDSL interfaces.

**Example** `set parallel-dialing = 12`

**Location** `SYSTEM`

### parent-node-index

**Description** Specifies the number identifying the node that will represent this peer group at the next higher routing level, if this node becomes peer group leader (PGL).

**Usage** The default 0 (zero) value indicates that no parent node exists.

**Example** `set parent-node-index = 0`

**Location** `PNMI-NODE-CONFIG:node-pgl`

## partial-packet-discard

**Description** Specifies whether the remaining cells in a packet (except the last cell) are to be discarded if buffers become congested after some cells of a packet have been queued.

**Usage** Valid values are as follows:

- **yes**—Specifies that the remaining cells in a packet (except the last cell) are discarded if buffers become congested after some cells of a packet have been queued. In addition, if congestion occurs when the unit is receiving the last cell of a packet, it discards the entire next packet. Partial packet discard (PPD) relies on a higher layer to reject the partial packet when it is received.
- **no** (the default)—Specifies that none of the remaining cells in a packet are discarded if buffers become congested after some cells of a packet have been queued.

**Dependencies** This parameters applies only to ATM adaptation layer 5 (AAL5) circuits.

**Location** ATM-QOS

## password

**Description** Specifies a password.

- In a user profile, the `password` setting specifies a password that the user must enter to log in.
- In a `tunnel-options` subprofile configured for Ascend Tunnel Management Protocol (ATMP), the `password` setting specifies the password that a Foreign Agent must supply to establish a tunnel with the Stinger router module.
- In an `snmpv3-usm-user` profile, the `password` setting specifies the user's password, which maps to a 16-octet or 20-octet key, in compliance with RFC 2574.

**Usage** Specify a text string of up to 20 characters. The default is null. The value you enter is case sensitive.



**Note** In an `snmpv3-usm-user` profile, 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 !`

**Example** `set password = unit`

**Dependencies** Consider the following:

- You must set `agent-mode` to `home-agent` for the `password` setting to apply in a `tunnel-options` subprofile.
- In an `snmpv3-usm-user` profile, you must specify a password if the `auth-protocol` setting is a value other than `no-auth`.

**Location** ATMP  
CONNECTION:tunnel-options  
SNMPV3-USM-USER  
USER

### *password-enabled*

**Description** Specifies whether all failed Telnet login attempts generate a trap (notification).

**Usage** Valid values are as follows:

- **yes**—Specifies that all failed Telnet login attempts generate a trap. This is the default.
- **no**—Specifies that failed Telnet login attempts do not generate a trap.

**Example** set password-enabled = no

**Dependencies** When password-enabled is set to yes, you must also set security-enabled to yes for all failed Telnet login attempts to generate a trap.

**Location** TRAP

### *password-for-direct-access*

**Description** *Not used.*

**Location** TERMINAL-SERVER:dialout-configuration

### *password-prompt*

**Description** *Not used.*

**Location** TERMINAL-SERVER:terminal-mode-configuration

### *path-state*

**Description** Read-only. Indicates the state of the synchronous optical network (SONET) path.

**Usage** The path-state value is read-only.

**Example** path-state = sonet-path-active-no-defect

**Location** OC3-ATM-STAT

## pattern-test-status

**Description** Read-only. Indicates the result of the pattern test.

**Usage** The pattern-test-status value is read-only. Valid values are as follows:

- none—Indicates that no pattern test has been run on this link.
- in-sync—The pattern test indicates that the line is synchronized.
- lost-sync—The pattern test indicates that the line has lost synchronization.

**Location** DS1-ATM-STAT

## p-bit-error-count

**Description** Read-only. Indicates the number of P-bit parity errors received in Asynchronous Transfer Mode (ATM) error-checking since the last time the unit was reset.

P-bit errors indicate that the unit received a P-bit code on the DS3 M-frame that differs from the locally calculated code.

**Usage** The p-bit-error-count value is read-only.

**Example** p-bit-error-count = 0

**Location** DS3-ATM-STAT  
E3-ATM-STAT

## pcm-mode

**Description** *Not currently used.* Specifies the number of active channels in a pulse code modulation (PCM) highway.

**Usage** Valid values are the following:

- isdn—Use 23 channels to carry the cells.
- clear-channel (the default)—Use 24 channels to carry the cells.

**Example** set pcm-mode = isdn

**Location** DS1-ATM:line-config

## peak-cell-rate-cells-per-sec

**Description** Indicates peak cell rate (PCR), which is the maximum number of cells allowed per second.

**Usage** Specify a value within the range from 0 to 353207 CPS. The default value is 37 CPS. The value of this field is user-writable only if the system profile atm-qos-rate-unit parameter is set to cps.

**Example** set peak-cell-rate-cells-per-sec = 200

**Location** ATM-QOS

## peak-rate

**Description** Specifies the maximum effective bit rate allowed, in kilobits per second.

The Stinger unit verifies that the `peak-rate` value of a shaper does not exceed the effective line rate.

**Usage** The valid range is 1 through 135631. The default is 1000 (1Mbps).

**Example** `set peak-rate = 15000`

**Location** `SYSTEM:traffic-shapers`  
`ATM-INTERNAL:traffic-shapers n`

## peak-rate-kbits-per-sec

**Description** Specifies the peak bit rate per second in kilobits per second.

**Usage** Specify a value within the range from 0 to 149760Kbps. The default value is 16Kbps. The value of this field is user-writable only if the `system` profile `atm-qos-rate-unit` parameter is set to `kbps`. Use a value that is appropriate for the type of traffic, as follows:

- For constant bit rate (CBR) traffic, specify the static bit rate.
- For available bit rate (ABR), specify the maximum explicit rate.
- For variable bit rate (VBR), specify the upper boundary of the variable bit rate.

**Example** `set peak-rate-kbits-per-sec = 20`

**Location** `ATM-QOS`

## peer-delayed-ack-interval

**Description** In Private Network-to-Network Interface (PNNI), specifies the minimum amount of time between transmissions of delayed PNNI topology state element (PTSE) acknowledgement packets.

**Usage** Specify an integer in 100ms units. The default is 10.

**Example** `set peer-delayed-ack-interval = 10`

**Location** `PNNI-NODE-CONFIG:node-timer`

## perm-conn-upd-mode

**Description** Specifies under what circumstances the Stinger unit performs nonintrusive remote updates of the configurations of permanent connections.

**Usage** Valid values are as follows:

- **all** (the default)—Specifies that, if they are fetched from the RADIUS server, all existing permanent connections are torn down and reestablished following the update. This setting causes a service interruption every time any dedicated (nailed profile is updated or added.
- **changed**—Specifies that only changed permanent connections are torn down and reestablished.

**Example** `set perm-conn-upd-mode = changed`

**Location** `SYSTEM`

## pf-comp-enabled

**Description** *Not used.* Enables or disables protocol field compression. Asynchronous only.

**Location** `CONNECTION:ppp-options`

## phone-number

**Description** *Not currently used.* Specifies the number the Stinger unit dials to reach the switch.

**Usage** Specify a telephone number of up to 24 characters, limited to the following choice of characters: 1234567890()[!z-\*]. The default is null.

**Example** `set phone-number = 555-1234`

**Dependencies** For frame relay, if a dedicated (nailed-up) data link connection is in use, `phone-number` does not apply.

**Location** `CALL-INFO`  
`CALL-ROUTE`  
`FRAME-RELAY`

## phs-support

**Description** Read-only. Indicates whether support for the Personal Handyphone System (PHS) is enabled.

**Usage** The `phs-support` setting is read-only. Valid values are as follows:

- **yes**—Indicates that PHS support is enabled.
- **no**—Indicates that PHS support is disabled.

**Example** `phs-support = yes`

**Location** `BASE`

## *physical-address*

**Description** Identifies the location of a physical interface or module within the Stinger unit.

This value is used by the system to retrieve the configuration of an item. The system also addresses the Asynchronous Transfer Mode (ATM) internal interface of an ISDN digital subscriber line (IDSL) or router module by a *physical-address* value. The address has the format {shelf slot item}. The elements of the address are identified as follows:

- *shelf*—Currently, in Stinger units, the shelf number is always 1.
- *slot*—Number of the slot in which the module resides.
- *item*—Number of the interface on the module. Interfaces are numbered starting with 1 for the topmost or leftmost interface on the module. An item number of 0 (zero) denotes the entire slot.

**Usage** The *physical-address* setting is a complex field consisting of *shelf*, *slot*, and *item-number* component settings. This value is set by the system when it creates the profile for an interface. After you configure an interface and write the profile, you can clone the configuration by modifying this value, as shown in the following example.

**Example** The following example modifies the slot value to copy the configured profile for a module in another slot:

```
admin> set physical-address slot = 4
```

**Example** To specify an alarm event that will be triggered only when it occurs on the host itself, specify shelf 1. For example:

```
admin> set physical-address shelf = shelf-1
```

**Example** To configure an alarm for a specific remote shelf, specify the ID of that shelf. For example, to configure an alarm for shelf 2:

```
admin> set physical-address shelf = shelf-2
```

**Location** This parameter appears in every profile associated with one of the system's physical interfaces:

```
ALARM
AL-DMT
AL-DMT-STAT
ATM-INTERNAL
ATM-INTERNAL-STAT
CARD-CODE
DEBUG
DS1-ATM
DS1-ATM-STAT
DS3-ATM
DS3-ATM-STAT
```



E3-ATM  
 E3-ATM-STAT  
 HDLSL2  
 HDLSL2-STAT  
 HIGH-SPEED-SLOT-STATIC-CONFIG  
 IDSL  
 IMA-GROUP-STAT  
 IMAHW-CONFIG  
 IP-INTERFACE:interface-address  
 LIM-SPARING-CONFIG  
 LINE-DIAG  
 LINE-DIAG-STAT  
 LINE-TESTS  
 MODEM  
 OC3-ATM  
 OC3-ATM-STAT  
 REMOTE-SHELF-STAT:host-port  
 SDSL  
 SDSL-STAT  
 SERIAL  
 SHDSL  
 SHDSL-STAT  
 SLOT-STATIC-CONFIG  
 SWITCH-CONFIG:atm-parameters:outgoing-queue

## ping

**Description** *Not used.*

**Location** `TERMINAL-SERVER:terminal-mode-configuration`

## planned-bitrate-down

**Description** Specifies the constant bit rate for downstream traffic when operator-controlled rate-adaptive mode is in effect.

**Usage** Specify an integer from 0 to 1500Kbps. The default value is 1000Kbps.

**Example** `set planned-bitrate-down = 100`

**Dependencies** Consider the following:

- `planned-bitrate-down` does not apply when automatic-at-startup rate adaptation is in use on the line.
- If you set `planned-bitrate-down` to a nonzero value in one subprofile, set `planned-bitrate-down` to 0 (zero) in the other subprofile.

**Location** `AL-DMT:fast-path-config`  
`AL-DMT:interleave-path-config`

## planned-bitrate-up

**Description** Specifies the constant bit rate for upstream traffic when operator-controlled rate-adaptive mode is in effect.

**Usage** Specify an integer from 0 to 2000Kbps. The default value is 512Kbps.

**Example** `set planned-bitrate-up = 100`

**Dependencies** Consider the following:

- `planned-bitrate-up` does not apply when automatic-at-startup rate adaptation is in use on the line.
- If you set `planned-bitrate-up` to a nonzero value in one subprofile, set `planned-bitrate-up` to 0 (zero) in the other subprofile.

**Location** `AL-DMT:fast-path-config`  
`AL-DMT:interleave-path-config`

## pnni-enabled

**Description** Read-only. Indicates the status of the Private Network-to-Network Interface (PNNI) protocol feature.

**Usage** Read-only parameter with the following possible values:

- `yes` (the default)—PNNI feature is enabled.
- `no`—PNNI feature is not enabled.

**Example** `pnni-enabled = yes`

**Location** `BASE`

## pnni-link-state

**Description** Read-only. Indicates the Private Network-to-Network Interface (PNNI) link state of the port.

**Usage** This parameter is read-only. Valid values are as follows:

- `not-configured`—No link state has been configured for the port.
- `up`—Link state for the port is up.
- `down`—Link state for the port is down.

**Example** `pnni-link-state = up`

**Location** `ATM-IF-STAT`

## pnni-scope

**Description** Specifies the extent of the advertisement of reachability from the advertising Private Network-to-Network Interface (PNNI) node to the address prefix.

**Usage** The default value is 0.

**Example** `set pnni-scope = 0`

**Location** `PNNI-ROUTE-ADDR`

## poll-after-retransmission

**Description** Specifies whether the Stinger unit sends a poll after retransmitting protocol data units (PDUs) before sending any further PDUs.

**Usage** Valid values are as follows:

- `yes`—Enables the poll.
- `no` (the default)—Disables the poll.

**Example** `poll-after-retransmission = yes`

**Location** `ATM-IF-SIG-PARAMS:qsaal-options`

## poll-inact-factor

**Description** Number of consecutive polls on the interface for which no Integrated Local Management Interface (ILMI) response message is received before ILMI connectivity is considered lost. *ILMI is not supported with the current software version.*

**Usage** Specify a value from 1 to 65536. The default value is 4.

**Example** `set poll-inact-factor = 12`

**Location** `ATM-IF-CONFIG:extension-config`

## poll-interval

**Description** Specifies the interval in seconds at which to send Hello packets to a neighboring router that has become inactive.

**Usage** Specify an integer. A value of 0 (zero) specifies that no Hello packets are sent to a neighboring router from which no Hello packets have been received for the number of seconds specified in the `dead-interval` setting. If you specify a nonzero value, use a larger value than the normal `hello-interval` default. The default value is 10.

**Example** `set poll-interval = 120`

**Location** `CONNECTION:ip-options:ospf-options`  
`IP-INTERFACE:ospf`

## pool-base-address

**Description** Specifies the base addresses of up to 128 IP address pools. A contiguous block of addresses must be available, starting with the address you specify.

**Usage** For each pool, specify the base IP address of a block of contiguous addresses. The default is 0.0.0.0.



**Caution** For Point-to-Point Protocol (PPP) interfaces, the Windows operating system uses a default subnet mask of /24. Therefore, if NetBIOS over IP is enabled, connected Windows users will broadcast to .255, causing a performance problem for anyone connected at that address.

**Example** `set pool-base-address[3] = 10.207.23.1`

**Dependencies** Consider the following:

- An address in a pool does not accept a subnet mask modifier, because pool addresses are advertised as host routes. If you allocate IP addresses on a separate IP network or subnet, make sure you inform other IP routers about the route to that network or subnet.
- The number of addresses in the pool must be specified by `assign-count`.
- If you are using network summarization (by means of the `pool-summary` setting), the address you specify must be network aligned.
- In a `vrouter` profile, the address pool is exclusive to one virtual router (VRouter). If you do not specify an address pool in a `vrouter` profile, virtual routers can share the address pools defined in the `ip-global` profile.
- If you change the value of `pool-base-address` to a lower number, you must reset the unit for the change to take effect.

**Location** IP-GLOBAL

VROUTER

## pool-chaining

**Description** Enables or disables IP pool chaining.

**Usage** Valid values are as follows:

- `yes`—Enables pool chaining. The system treats contiguous IP address pools as a single extended pool space when searching for an available address to assign to a caller.
- `no` (the default)—Disables pool chaining.

**Example** `set pool-chaining = yes`

**Dependencies** Consider the following:

- Address pools must be defined either locally or in RADIUS pseudo-user profiles.
- When specified in a `vrouter` profile, address pools are exclusive to that virtual router. If address pools are not specified in a `vrouter` profile, the virtual router(s) can share the address pools defined in the `ip-global` profile.

**Location** IP-GLOBAL

VROUTER

---

## pool-name [n]

**Description** Assigns a name to an IP address pool for TACACS+ authentication or virtual router (VRouter) operation.

**Usage** Specify a name of up to 11 characters. The default is null.

**Example** set pool-name 1 = newyork

**Dependencies** Consider the following:

- Each pool configuration consists of a base address (specified by pool-base-address), address count (specified by assign-count), and name (specified by pool-name).
- If TACACS+ authentication is not in use, the Stinger unit treats a pool name specification as a comment.
- In a vrouter profile, the address pool is exclusive to one virtual router. If you do not specify an address pool in a vrouter profile, virtual routers can share the address pools defined in the ip-global profile.

**Location** IP-GLOBAL  
VROUTER

## pool-ospf-adv-type

**Description** Specifies how to import summarized pool addresses into Open Shortest Path First (OSPF).

**Usage** Valid values are as follows:

- type-1 (the default)—Instructs the Stinger unit to import the pool addresses into OSPF as external type 1 routes.
- type-2—Instructs the Stinger unit to import the pool addresses into OSPF as external type 2 routes.
- internal—Instructs the Stinger unit to import the pool addresses into OSPF as intra-area routes.

**Example** set pool-ospf-adv-type = type-2

**Dependencies** For pool-ospf-adv-type to apply, you must set pool-summary to yes and enable OSPF.

**Location** IP-GLOBAL

## pool-summary

**Description** Sets or clears the pool summary flag. The use of pool summarization can significantly reduce the size of routing table advertisements.

When the flag is set, the Stinger unit adds IP addresses from an address pool to the routing table as individual host routes, and summarizes the series of host routes into a network route advertisement. It advertises the entire pool as a route, and only privately keeps track of the IP addresses in the pool. If a remote network sends a packet to an inactive IP address, the Stinger unit either bounces the packet back to the remote network or silently discards it.

When specified in a `vrouter` profile, address pools are exclusive to that virtual router. If address pools are not specified in a `vrouter` profile, the virtual router(s) can share the address pools defined in the `ip-global` profile.

**Usage** Valid values are as follows:

- `yes`—Enables pool summarization.
- `no` (the default)—Disables pool summarization.

**Example**

```
set pool-summary = yes
set pool-base-address [3] = 10.12.253.1
set assign-count = 62
```

**Dependencies** When `pool-summary` is set to `yes`, the `pool-base-address` you specify must be network aligned.

**Location** `IP-GLOBAL`  
`VROUTER`

## port

**Description** Specifies or indicates the port number, as follows:

- In the `tcp-clear-options` subprofile of a `connection` profile, `port` specifies the first port to which a TCP-Clear session attempts to connect. You can specify a port on up to three more login hosts with the parameters `port2`, `port3`, and `port4`.  
  
If the TCP connection to the first specified host-port combination fails, the system attempts to connect to the next specified host and port. If the connection to the next host-port combination fails, the system attempts to connect to the third host and port, and so forth. If all connection attempts fail, the session terminates and the Stinger unit returns a TCP connection error to the dial-in client.
- In the `terminal-server` profile, `port` specifies the port on the login host to which the user connects in immediate mode.
- In a `log` profile and `auxiliary-syslog` subprofile, `port` specifies the destination port of the syslog host.
- In a `vcc-members` or `vcc-ident` subprofile, `port` indicates the port number of the module that owns the virtual channel connection (VCC) on an Asynchronous Transfer Mode (ATM) link.

**Usage** Specify a port number. Defaults are as follows:

- For a tcp-clear-options subprofile of a connection profile, the default is 0 (zero).
- For a terminal-server profile, the default is 0 (zero).
- For the log profile, the default is 514.

For a vcc-members or vcc-ident subprofile, the port setting is read-only.

**Dependencies** Consider the following:

- The port value in the log profile affects all data streams.
- The port 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.

**Location** ATMPVC-STAT:vcc-members:vcc-members [n]

ATMVCC-STAT:vcc-ident

CONNECTION:tcp-clear-options

LOG

LOG:auxiliary-syslog:auxiliary-syslog [n]

TERMINAL-SERVER:immediate-mode-options

port2

port3

port4

**Description** Specifies a port on up to three login hosts, in addition to the first specified by port, to which a TCP-Clear session attempts to connect.

You can specify one port for each of four login hosts. If the TCP connection to the first specified host-port combination fails, the system attempts to connect to the next specified host and port. If the connection to the next host-port combination fails, the system attempts to connect to the third host and port, and so forth. If all connection attempts fail, the session terminates and the Stinger unit returns a TCP connection error to the dial-in client.

**Usage** Specify a port number. The default is 0 (zero).

**Example** The following example specifies two login host-port combinations:

```
admin> read connection fred
CONNECTION/fred read
admin> set tcp-clear-options host = mercury
admin> set tcp-clear-options host2 = venus
admin> set tcp-clear-options port = 155
admin> set tcp-clear-options port2 = 256
admin> write
CONNECTION/fred written
```

**Location** CONNECTION:tcp-clear-options

### port-1-shelf

**Description** The shelf ID of the remote shelf directly connected to the first cascade port on the host.

**Usage** This parameter is read-only.

**Example** port-1-shelf = 1

**Location** REMOTE-SHELF-STAT:topology

### port-2-shelf

**Description** The shelf ID of the remote shelf directly connected to the second cascade port on the host.

**Usage** This parameter is read-only.

**Example** port-1-shelf = 2

**Location** REMOTE-SHELF-STAT:topology

### port-activation-array

**Description** An array selecting a specific port or ports on a line interface module (LIM) to be isolated for galvanic isolation tests, or connected to a tone generator for multiport tone tests.

**Usage** Valid values are as follows:

- yes—Isolates the port or connects it to a tone generator.
- no (the default)—Does not isolate or connect the port.

**Example** The following commands select ports 3 and 9 for testing:

```
set port-activation 3 = yes
```

```
set port-activation 9 = yes
```

**Dependencies** This parameter is valid only if `specific-ports` is set to `yes`.

**Location** LINE-TESTS

### port-block-enabled

**Description** Enables or disables port blocking to prevent traffic flows between subscriber interfaces in the same VLAN.

**Usage** Valid values are as follows:

- yes—A “router” VLAN interface must be designated by setting the `lan-router-interface-address` parameter. This is the default value.
- no—Disable port blocking.



**Example** `set port-block-enabled = no`

**Location** BRIDGE-GROUP

## port-cac-enable

**Description** Enable/disable connection admission control (CAC) on the line interface module's (LIM) ports.

**Usage** Valid values are as follows:

- `yes`—CAC on the LIM's ports is enabled.
- `no` (the default)—CAC on the LIM's ports is disabled.

**Example** `set port-cac-enable = yes`

**Location** SLOT-STATIC-CONFIG

## port-cac-oversubscription

**Description** Specifies oversubscription to the port provisioned bandwidth.

**Usage** Integer value from 0 to 10,240. The default value is 10.

**Example** `set port-cac-oversubscription = 5000`

**Location** SLOT-STATIC-CONFIG

## port-enabled

**Description** Specifies whether the Stinger unit traps changes in the state of a host interface and sends trap (notification) protocol data units (PDUs) to the Simple Network Management Protocol (SNMP) manager.

All port connections are monitored in a *state machine* and reported by means of this trap.

**Usage** Valid values are as follows:

- `yes`—Specifies that the Stinger unit sends trap PDUs to the host specified by `host-address`.
- `no`—Specifies that the Stinger unit does not send trap PDUs. This is the default.

**Example** `set port-enabled = yes`

**Location** TRAP

## port-for-direct-access

**Description** *Not used.*

**Location** TERMINAL-SERVER:dialout-configuration

## port-num

**Description** Read-only. Identifies a trunk port within the system.

**Usage** The port-num value is read-only and has a maximum of 15 characters.

**Example** port-num = 1:17:1

**Location** HIGH-SPEED-SLOT-STATIC-CONFIG:trunk-cac-config



**Note** This parameter was previously located in the atm-config profile. Its use in that location has been deprecated.

## port-number

**Description** Specifies the port number to be redirected.

**Usage** Specify a numeric value in a range of 0 to 65535. The default value is 0.

**Example** set port-number = 23

**Location** CONNECTION:port-redirect-options

## port-state

**Description** Read-only. Indicates the state of the physical port.

**Usage** Valid values for this read-only parameter are as follows:

- not-configured—The port is not configured.
- up—The port is in an up state.
- down—The port is in a down state.

**Example** port-state = up

**Location** ATM-IF-STAT

## port-status

**Description** Read-only. An array showing the line-test status of each port on a line interface module (LIM).

**Usage** This array is a read-only field. A value equal to the slot number of the LIM indicates that a port is isolated or connected to a tone generator. A value of 0 indicates that a port is not isolated or connected to a tone generator.

**Location** LINE-TESTS

## port-towards-host-shelf

**Description** The port on the remote shelf used for the link to the host.

**Usage** This parameter is read-only.

**Example** `port-towards-host-shelf = remote-shelf-cascade-port-none`

**Location** `REMOTE-SHELF-STAT:topology`

## post-end

**Description** Read-only, Indicates the time at which this controller detected the end of a remote power-on self test (POST).

**Usage** This read-only parameter has a numeric range of 0 to 4294967295.

**Example** `post-end = 123`

**Location** `REDUNDANCY-STATS:context-stats`

## post-start

**Description** Read-only, Indicates the time at which this controller started local power-on self test (POST).

**Usage** This read-only parameter has a numeric range of 0 to 4294967295.

**Example** `post-start = 123`

**Location** `REDUNDANCY-STATS:context-stats`

## power-supply-enabled

**Description** Specifies whether the system generates a trap (notification) when a power supply module is added or removed.

**Usage** Valid values are as follows:

- **yes**—Specifies that the system generates a trap when a power supply module is added or removed. This is the default.
- **no**—Specifies that the system does not generate a trap when a power supply module is added or removed.

**Example** `set power-supply-enabled = no`

**Location** `TRAP`

## ppp-circuit

**Description** Specifies whether transparent Point-to-Point Protocol (PPP) switching is enabled on the Stinger unit.

**Usage** Valid values are as follows:

- `none`—Transparent PPP switching disabled. This is the default.
- `transparent`—Transparent PPP switching is enabled.

**Example** `set ppp-circuit = none`

**Location** `CONNECTION:ppp-options`

## ppp-circuit-name

**Description** Specifies the name of a Point-to-Point Protocol (PPP) circuit.

A PPP transparent circuit consists of two linked connections. You configure the connections by setting `ppp-circuit` to `transparent`, which enables the interface to be part of the PPP circuit.

**Usage** Specify an ASCII string with a maximum length of 15 characters. The default is a null string. Characters are limited to the character set that is used for the frame relay circuit name. Note that encapsulation must be `ppp`. You link the connections together by specifying the same `ppp-circuit-name` value for the two connections that form the PPP circuit.

**Example** `set ppp-circuit-name = firstpppcircuit`

**Dependencies** Consider the following:

- This parameter is ineffective unless `ppp-circuit` parameter is set to `transparent`.
- For IDSL, if you do not specify a circuit name the Stinger unit creates a circuit name based on the values of the VPI, Vci, and Nailed-Group parameters set in the ATM-Connect-Options subprofile. If you specify a circuit name, it overrides the default name created by the Stinger unit.

**Location** `CONNECTION:ppp-options`

## pppoe

**Description** Enables or disables processing of PPP over Ethernet (PPPoE) packets on a Stinger interface.

- When PPPoE is enabled on an interface, PPPoE requests received on the interface are handled by the onboard PPPoE server in the router module.
- If PPPoE is not enabled on an interface and bridging is enabled, the router module bridges the PPPoE requests to an external PPPoE server.

**Usage** Specify `yes` or `no`. The default value is `no`.

- `no`—Enable PPPoE packet processing on the interface.
- `yes`—Disable PPPoE packet processing on the interface.

**Example** `set pppoe = yes`

**Dependencies** If both PPPoE and packet bridging are disabled on the Ethernet interface, PPPoE packets will be discarded. Under those conditions, only IP packets will be accepted on the interface.

**Location** CONNECTION:pppoe-options  
ETHERNET:pppoe-options

## precedence

**Description** Specifies the priority level of the data stream. The three most significant bits of the type-of-service (TOS) byte are priority bits used to set precedence for priority queuing.

When TOS is enabled in a connection profile, you can set the priority bits to one of the following values to set proxy-quality-of-service (QoS) precedence for the traffic on a particular WAN connection. In a filter profile, specifying a precedence value causes the system to enable proxy-QoS for packets that match the filter.

**Usage** Specify one of the following values (most significant bit first):

- 000 (the default)—Normal priority
- 001—Priority level 1
- 010—Priority level 2
- 011—Priority level 3
- 100—Priority level 4
- 101—Priority level 5
- 110—Priority level 6
- 111—Priority level 7 (the highest priority)

**Example** `set precedence = 001`

**Dependencies** For this setting to apply, TOS and IP routing must be enabled in the connection profile, or TOS must be specified as the filter type in the filter profile.

**Location** CONNECTION:ip-options:tos-options  
FILTER:input-filters[n]:tos-filter  
FILTER:output-filters[n]:tos-filter

## preempt

**Description** Specifies the number of seconds of idle time that a session can have before being preempted.

**Usage** Specify a numeric value in seconds in a range of 0 to 65535. The default value is 60 (1 minute). The value 0 (zero) prevents preemption.

**Example** `set preempt = 100`

**Dependencies** The idle-timer parameter must be greater in value than preempt.

**Location** CONNECTION:session-options

## preference

**Description** Specifies a preference value for the route. When choosing a route, the router first compares their preference values, preferring the lowest number. If the preference values are equal, the router compares the metric values, and selects the route with the lowest metric.

**Usage** Specify a number from 0 to 255. A value of 255 prevents the use of the route, and is valid only for a WAN route specified by a connection profile. Following are the default preferences for different types of routes:

- 0 (zero)—Connected routes
- 10—Open Shortest Path First (OSPF) routes
- 30—Routes learned from Internet Control Message Protocol (ICMP) redirects
- 100—Routes learned from RIP
- 100—Static routes
- 100—Ascend Tunnel Management Protocol (ATMP) routes

**Example** `set preference = 100`

**Location** CONNECTION:ip-options  
IP-ROUTE

## prefix-len

**Description** Specifies the length of the reachable Asynchronous Transfer Mode (ATM) address prefix.

**Usage** Specify a number from 0 to 152.

**Example** `set prefix-len = 50`

**Location** PNNI-ROUTE-ADDR  
PNNI-SUMMARY-ADDR:addr-index

## prefix-name

**Description** Name of the atm-prefix profile. The profile with the default index contains the system-generated prefix and can be used to generate defaults for all three types of system addresses.

**Usage** Enter up to 20 alphanumeric characters to specify the name of the profile. The default value is default.

**Example** `set prefix-name = atm-pre-1`

**Location** ATM-PREFIX

## previous-trunk-daughter-type

**Description** Specifies the previous type of trunk daughter module in this device, if there was one.

**Usage** Valid values are as follows:

- trunk-daughter-none
- trunk-daughter-oc3-quad
- trunk-daughter-ds3
- trunk-daughter-oc3-ds3-combo
- trunk-daughter-oc3-single
- trunk-daughter-ds3-single
- trunk-daughter-e3
- trunk-daughter-e3-single

**Example** set previous-trunk-daughter-type = trunk-daughter-e3

**Location** TRUNK-DAUGHTER-DEV

## primary-preference

**Description** In a redundant system, specifies the preference level for electing this control module as primary at the next system reset.

**Usage** Valid values are as follows:

- no-preference (the default)—Specifies that the system chooses the primary control module. The system chooses the one that was primary most recently.
- first-controller-preferred—Specifies that the system gives preference to the control module in the first control module slot (slot 8). If this control module is not available, the system designates the one in slot 9 as primary.
- second-controller-preferred—Specifies that the system gives preference to the control module in the second control module slot (slot 9). If this control module is not available, the system designates the one in slot 8 as primary.

**Example** set primary-preference = first-controller-preferred

**Location** REDUNDANCY

## primary-sdtn-empty-enabled

**Description** Specifies whether the short-duration transaction network (SDTN) primary list empty trap (notification) is enabled.

**Usage** Valid values are as follows:

- yes—Specifies that the SDTN primary list empty trap is enabled. This is the default.
- no—Specifies that the SDTN primary list empty trap is not enabled.

**Example** `set primary-sdtn-empty-enabled = no`

**Location** `TRAP`

## `primary-tunnel-server`

**Description** Specifies the IP address or hostname of the Ascend Tunnel Management Protocol (ATMP) primary Home Agent, L2TP Network Server (LNS) end point, or intermediate destination that decapsulates IP packets using IP-within-IP (IPIP) tunneling.

**Usage** Specify an IP address in dotted decimal notation, or a symbolic hostname containing up to 31 characters. The IP address must be the system address, not the IP address of the interface on which the unit receives tunneled data. The default is 0.0.0.0.

If you specify a hostname, the Stinger router module uses the Domain Name System (DNS) to look up the host IP address. If the unit requires a UDP port number different from the value specified by `udp-port`, you can specify a port value by appending a colon character (:) and the port number to the IP address or hostname.

**Example** The following setting specifies an IP address and UDP port number:

```
admin> set primary-tunnel-server = 10.11.22.33:8877
```

The following setting specifies a hostname and UDP port number:

```
admin> set primary-tunnel-server = server.company.com:6969
```

**Dependencies** You must set `profile-type` to `mobile-client` for the `primary-tunnel-server` setting to apply.

**Location** `CONNECTION:tunnel-options`

## `prior-function`

**Description** Read-only. Indicates the prior function of the controller in this context.

**Usage** Read-only parameter with the following possible values:

- `no-function`
- `primary`
- `secondary`

**Example** `prior-function = primary`

**Location** `REDUNDANCY-STATS:context-stats`



## priority

**Description** Specifies a priority, as follows:

- For the `ospf-options` and `ospf` subprofiles, specifies the priority of the Open Shortest Path First (OSPF) router with regard to designated-router and backup designated-router election.
- For the `txlink-config` subprofile, specifies the priority assigned for the timing reference link (TRL). The TRL is used to derive the inverse multiplexing over ATM (IMA) data cell rate (IDCR).

**Usage** Valid values are as follows:

- For the `ospf-options` and `ospf` subprofiles, specify an integer. In a connection profile or `ip-interface` profile, the Stinger unit can function as either a designated router or backup designated router. However, many sites choose to assign these functions to LAN-based routers to dedicate the Stinger unit to WAN processing. The default is 5
- For the `txlink-config` subprofile, specify a numeric value between 0 and 7.

**Example** `set priority = 4`

**Dependencies** For OSPF applications, choose the designated-router and backup designated-router election priority on the basis of each device's processing power and reliability. Assigning a priority of 1 or greater places the Stinger unit on the list of possible designated routers and backup designated routers. A priority value of 0 (zero) excludes the unit from becoming a designated router or backup designated router. The higher the priority value of the Stinger unit relative to other OSPF routers on the network, the better are the chances that it will become a designated router or backup designated router.

**Location** `DS1-ATM:line-config:ima-option-config:txlink-config`  
`CONNECTION:ip-options:ospf-options`  
`IP-INTERFACE:ospf`

## priority-number

**Description** Read-only. Indicates the number of the traffic shaper.

**Usage** Read-only numeric value, set to the number of the traffic shaper.

**Example** `priority-number = 16`

**Location** `SYSTEM:traffic-shapers`  
`ATM-INTERNAL:traffic-shapers [n]`

## private-route

**Description** Enables or disables advertisement of the route in RIP update packets sent out by the system.

**Usage** Valid values are as follows:

- **yes**—Excludes the route from update packets.
- **no** (the default)—Includes the route in RIP updates.

**Example** `set private-route = yes`

**Location** CONNECTION:ip-options  
IP-ROUTE

## private-route-profile-required

**Description** Specifies whether the system must have access to a private routing table to establish a call.

- In a connection profile, this parameter specifies whether access to the private routing table is required for the session. This parameter does not apply if the profile does not refer to a private routing table by name.
- In the answer-defaults profile, this parameter is used for RADIUS user profiles that refer to a private routing table and do not specify a value for Ascend-Private-Route-Required (55).

**Usage** Valid values are as follows:

- **yes**—Drops the call if the system cannot locate the private routing table.
- **no** (the default)—Establishes the link even if the system cannot locate the private routing table.

**Example** `set private-route-profile-required = yes`

**Dependencies** The system uses the private-route-profile-required value in the answer-defaults profile only if the Ascend-Private-Route-Required (55) attribute is not set in a RADIUS private-route profile.

**Location** ANSWER-DEFAULTS:ip-answer  
CONNECTION:ip-options

## private-route-table

**Description** Specifies the name of a private-route-table profile associated with the connection. The name can be that of a local profile or of a private-route pseudo-user profile in RADIUS.

**Usage** Specify the name of a private-route-table profile. The default is null.

**Example** `set private-route-table = private-rt-1`

**Dependencies** A local connection profile must use authentication, or it cannot point to a RADIUS private-route profile.

**Location** CONNECTION:ip-options

## priv-key

**Description** Specifies a privacy key for SNMPv3 user-based security model (USM) users.

**Usage** 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.

If you change the value of `priv-key` directly, keep in mind that the length of the escape sequence must be either of the following values:

- 10 (16d in hexadecimal) if message-digest algorithm 5 (MD5) is in use
- 14 (20d in hexadecimal) if the secure hash algorithm (SHA) is in use

If you specify an invalid value, the unit uses the previous key, if any, to communicate with the SNMP manager. If no previous key exists, this USM user cannot communicate with the network until a valid key is generated by means of the `snmpprivpass` command.

**Example** Suppose you use the `snmpprivpass` command to generate the following 16-byte string:

```
27 0a dc 75 f8 98 e5 7c 4c 03 22 7d dd ac 0d ef
```

The system displays it as the following `priv-key` value:

```
'\x0a\xdcu\xf8\x98\xe5|L\x03"\}\xdd\xac\x0d\xef
```

**Dependencies** Consider the following:

- You must generate the privacy key by means of the `snmpprivpass` command before the `snmpv3-usm-user` profile can be used for communication with the SNMP manager.
- If you change the authentication protocol from MD5 to SHA (or vice versa), you must change the privacy key by means of the `snmpprivpass` command. The previous protocol-and-key combination is used until you specify a new one.

**Location** SNMPV3-USM-USER

## priv-password

**Description** Specifies the privacy password for generating the private key for Data Encryption Standard (DES) encryption.

**Usage** Specify a text string. The default is null.

**Example** `set priv-password = homer`

**Dependencies** The `priv-password` parameter applies only if `priv-protocol` is set to `des-priv`.

**Location** `SNMPV3-USM-USER`

## `priv-protocol`

**Description** Specifies whether messages sent on behalf of the user to and from the Simple Network Management Protocol (SNMP) agent in the Stinger unit can be protected by encryption and, if so, the type of privacy protocol to be used.

**Usage** Valid values are as follows:

- `no-priv`—Specifies that no encryption is required and that privacy is disabled. This is the default.
- `des-priv`—Specifies that Data Encryption Standard (DES)-based privacy is required. Incoming messages that are DES-encrypted are interpreted. The Stinger system uses DES to encrypt outgoing responses. Note that outgoing reports are not encrypted.

**Example** `set priv-protocol = des-priv`

**Location** `SNMPV3-USM-USER`

## `profile`

**Description** Array that contains a listing of system profiles to which users in this user group are denied access.

**Usage** You can specify up to 400 profiles. The default setting for this array is null.

**Example** `set 1 = user`

**Location** `USER-GROUP`

## `profile-flags`

**Description** *Not used.*

**Location** `CONNECTION:answer-options'`

## `profile-required`

**Description** Specifies whether a dedicated profile is required to connect the user availing himself of this connection profile.

**Usage** Valid values are as follows:

- `yes`
- `no` (the default)

**Example** `set profile-required = yes`

**Location** `CONNECTION:answer-options`

## profiles-required

**Description** Specifies whether the Stinger unit rejects incoming calls for which it could find neither a connection profile nor an entry on a remote authentication server.

If you do not require a configured profile for all callers, the Stinger unit builds a temporary profile for unknown callers. Many sites consider the use of a temporary profile a security breach, and require that all callers have a configured profile.

**Usage** Valid values are as follows:

- **yes**—Specifies that the Stinger unit requires a configured profile for all callers. The unit rejects calls for which it cannot find a configured profile. This is the default.
- **no**—Specifies that if the Stinger unit cannot find a configured profile, it creates a temporary profile for the caller.

**Example** `set profiles-required = no`

**Dependencies** You cannot set `profiles-required` for terminal-server calls.

**Location** `ANSWER-DEFAULTS`

## profile-type

**Description** Specifies the type of tunneling profile.

**Usage** Specify one of the following values:

- **disabled**—The connection is not used for tunneling. This is the default.
- **mobile-client**—The profile is used to authenticate a mobile client. Use this setting for PPP clients using Layer 2 Tunneling Protocol (L2TP) or Ascend Tunnel Management Protocol (ATMP) tunneling.
- **gateway-profile**—The profile sets up a gateway connection to an ATMP home network. Use this setting in an ATMP Home Agent gateway profile.
- **dialout-profile**—*Not supported.*
- **lan**—The default value for OSPF routing on a GigE interface.
- **wan**—The default value for OSPF routing on an ATM Trunk interface.

**Example** `set profile-type = mobile-client`

**Location** `CONNECTION:tunnel-options`  
`IP-INTERFACE:ospf`

## prompt

**Description** Specifies a string that the Stinger unit uses as a command-line prompt.

**Usage** Specify a string of up to 15 characters. In a user profile, the default is an asterisk, which causes the Stinger unit to substitute the value of the profile's name upon successful login.

This parameter is not used in the `terminal-mode-configuration` profile.

**Example** set prompt = virginia>

**Location** TERMINAL-SERVER:terminal-mode-configuration  
USER

## prompt-format

**Description** *Not used.*

**Location** TERMINAL-SERVER:terminal-mode-configuration

## protection-channel

**Description** Read-only. Indicates the physical address of the protection channel.

**Usage** This read-only parameter shows the address in { shelf slot port } format.

**Example** protection-channel = { shelf-1 trunk-module-2 2 }

**Location** APS-STAT

## protection-channel-signal-degrade-exponent

**Description** Specifies the signal degrade exponent for the protection channel in automatic protection switching (APS).

**Usage** Specify a number from 5 through 9. The default is 6.

**Example** set protection-channel-signal-degrade-exponent = 7

**Location** APS-CONFIG

## protection-channel-signal-failure-exponent

**Description** Specifies the signal failure exponent for the protection channel in automatic protection switching (APS).

**Usage** Specify a number from 3 through 5. The default is 3.

**Example** set protection-channel-signal-failure-exponent = 4

**Location** APS-CONFIG

## protection-mode

**Description** Specifies or indicates the mode of linear automatic protection switching (APS), depending on the profile it appears in.

**Usage** Currently only linear APS 1+1 is supported. The value 1+1 is the default.

**Example** set protection-mode = 1+1

**Location** APS-CONFIG  
APS-STAT

## proto

**Description** Specifies the mechanism by which the advertising node learns of reachability to the address prefix.

**Usage** Valid values are as follows:

- other—The protocol is unspecified. This is the default.
- local—Specifies a local routing protocol such as Integrated Local Management Interface (ILMI). *ILMI is not supported with the current software version.*
- mgmt—Specifies a management protocol such as Simple Network Management Protocol (SNMP).
- pnmi—Specifies ATM Forum Private Network-to-Network Interface (PNNI) dynamic routing protocol.

**Example** set proto = other

**Location** PNNI-ROUTE-ADDR

## protocol

**Description** Specifies the protocol type of packets to be filtered or redirected, as follows:

- When specified in the port-redirect-options subprofile of a connection profile, the specified setting is used for port redirection. Port redirection enables you to redirect any TCP or UDP packet to a specified server on the basis of its protocol and port information.
- When specified in a filter profile, the system compares the protocol number you specify to the protocol number field in packets. A number of 0 (zero) matches all protocols. If you specify a nonzero number, the system compares it to the protocol field in each packet.

**Usage** Valid values are as follows.

- In a connection profile, specify one of the following values:
  - none (the default)—Disables port redirection.
  - udp—Redirects UDP packets received on the port specified in the port-number parameter to the address specified in the redirect-address parameter.
  - tcp—Redirects TCP packets received on the port specified in the port-number parameter to the address specified in the redirect-address parameter.
- In a filter profile, specify a nonzero protocol number to identify the type of protocol to be filtered. For a list of assigned protocol numbers, see RFC 1700, *Assigned Numbers*, by Reynolds, J. and Postel, J., October 1994.

**Example** Use these examples to help you:

- For FTP traffic, set protocol and port-number in port-redirect-options as follows:  

```
set protocol = tcp
set port-number = 21
```
- For Telnet traffic, set protocol and port-number in port-redirect-options as follows:  

```
set protocol = tcp
set port-number = 23
```
- For HTTP traffic, set protocol and port-number in port-redirect-options as follows:  

```
set protocol = tcp
set port-number = 80
```
- In a filter profile, the following command sets the protocol to be filtered to TCP:  

```
set protocol = 6
```

**Dependencies** Consider the following:

- For port redirection, both the protocol and port-number settings are required to define a type of packet to be redirected.
- In a filter, this setting applies only if type is set to ip-filter or tos-filter.

**Location** CONNECTION:port-redirect-options

FILTER:input-filters[n]:ip-filter

FILTER:output-filters[n]:ip-filter

FILTER:input-filters[n]:tos-filter

FILTER:output-filters[n]:tos-filter

## proxy-arp

**Description** Enables or disables Proxy Address Resolution Protocol (ARP), which causes the router module to respond as a proxy for remote hosts on the far end of the bridged IP routing (BIR) link when a local host issues an ARP request.

**Usage** Valid values are as follows:

- yes—Enables Proxy ARP.
- no (the default)—Does not enable Proxy ARP.

**Example**

```
set proxy-arp = yes
```

**Location** CONNECTION:bir-options



## proxy-mode

**Description** Enables or disables Proxy Address Resolution Protocol (ARP) responses for remote devices that are assigned local addresses.

**Usage** Valid values are as follows:

- off—Specifies that the system does not proxy any addresses. This is the default.
- active—Specifies that the system responds to an ARP request with its own media access control (MAC) address if the request matches an active connection profile over which the Stinger unit routes IP.
- inactive—Specifies that the system responds to an ARP request if the request matches the IP address of any inactive connection profile over which the unit routes IP.
- always—Specifies that the system responds to an ARP request with its own MAC address if the request matches any IP address to which the unit has a route.

**Example** set proxy-mode = inactive

**Location** IP-INTERFACE

## psbf-clear-timer-duration

**Description** Specifies the protection switching byte failure (PSBF) clear timer duration in tenths of milliseconds in automatic protection switching (APS).

**Usage** Specify a number from 0 through 4,294,967,295. The default is 1000.

**Example** set psbf-clear-timer-duration = 20

**Location** APS-CONFIG

## psbf-failure

**Description** Read-only. Indicates whether a protection switching byte failure (PSBF) occurred in the automatic protection switching (APS) system.

**Usage** Valid values for this read-only parameter are as follows:

- true—A protection switching byte failure (PSBF) occurred.
- false—No PSBF occurred.

**Example** psbf-failure = false

**Location** APS-STAT

## psbf-failure-timer-duration

**Description** Specifies the protection switching byte failure (PSBF) timer duration in tens of milliseconds in automatic protection switching (APS).

**Usage** Specify a number from 0 through 4,294,967,295. The default is 250.

**Example** set psbf-failure-timer-duration = 200

**Location** APS-CONFIG

## psd-frequency-level

**Description** Read-only. Reports test results concerning noise in a copper loop test (CLT).

**Usage** Valid values for this read-only parameter are as follows:

| Noise test type                                            | Data reported                                                                                                                                                                                                            |
|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Background noise test in power spectral density (PSD) mode | Data consists of 371 pairs of PSD test data. The first number in each pair is the test frequency in kilohertz. The second number in each pair is the noise level in decibels referred to 1 milliwatt per hertz (dBm/Hz). |
| Background noise test, E, F, or G mode                     | A single value representing aggregated noise in hundredths (0.01) of a dBm.                                                                                                                                              |
| Insertion loss test                                        | Data consists of 371 pairs of test data. The first number in each pair is the test frequency in kHz. the second number in each pair is the loss in hundredths (0.01) of a decibel.                                       |
| Signal-to noise-test                                       | Data consists of 371 pairs of test data. The first number in each pair is the test frequency in kilohertz. The second number in each pair is the S/N ratio in hundredths (0.01) of a decibel.                            |

**Example** psd-frequency-level = [ { 4 -7892 } { 9 -3849 } { 13 -3849 } { 17 -3422 } { 22 +

**Location** CLT-RESULT

## ptse-holddown

**Description** Specifies the initial value in 100-millisecond units for the Private Network-to-Network Interface (PNNI) topology state element (PTSE) hold-down timer.

The node uses this timer value to limit the rate at which it can send PTSEs.

**Usage** Specify a positive nonzero number. The default is 10.

**Example** `set ptse-holddown = 8`

**Location** PNNI-NODE-CONFIG:node-timer

## ptse-id-ptse-id

**Description** Read-only. Specifies the PNNI topology state element (PTSE) *identifier (ID)*. This ID is originated by the node that contains the information group(s) describing the reachable address.

**Usage** For reachable addresses learned by means other than PNNI, the default zero value is required.

**Example** `ptse-id-ptse-id = 0`

**Location** PNNI-Route-Addr

## ptse-lifetime-factor

**Description** Specifies the multiplier, expressed as a percentage, by which the system multiplies the `ptse-refresh-interval` value to obtain the initial lifetime to place into self-originated Private Network-to-Network Interface (PNNI) topology state elements (PTSEs).

**Usage** Specify a percentage by which the `ptse-refresh-interval` is multiplied. The product is assigned to self-originated PTSEs. The default is 200

**Example** `set ptse-lifetime-factor = 150`

**Location** PNNI-NODE-CONFIG:node-timer

## ptse-refresh-interval

**Description** Specifies the value, in seconds, for the Refresh timer. This value is used to determine how often to originate Private Network-to-Network Interface (PNNI) topology state elements (PTSEs) in the absence of triggered updates.

**Usage** Specify the number of seconds. The default is 1800.

**Example** `set ptse-refresh-interval = 1700`

**Location** PNNI-NODE-CONFIG:node-timer

## pvc-failure-intvl

**Description** Minimum number of seconds between the sending of PVC failure trap notifications.

**Usage** Set a value from 0 to 3600 seconds. The default value is 30.

**Example** `set pvc-failure-intvl = 60`

**Location** ATM-IF-CONFIG:extension-config

## pvc-failure-trap-enabled

**Description** Enables or disables generation of traps (notifications) in response to permanent virtual circuit (PVC) failures on this interface.

**Usage** The following values are valid:

- `no` (the default)—Disables traps in response to PVC failures.
- `yes`—Enables traps in response to PVC failures.

**Example** `set pvc-failure-trap-enabled = yes`

**Location** ATM-IF-CONFIG:extension-config

## pvc-type

**Description** Read-only. Indicates the type of permanent virtual circuit (PVC) in use on an Asynchronous Transfer Mode (ATM) connection.

**Usage** The PVC-Type value is read-only. Valid values are as follows:

- `connecting`—Indicates that the PVC is a point-to-point connection.
- `terminating`—Indicates that the PVC terminates on this platform.

**Location** ATMPVC-STAT

---

## Q

### qos-class

**Description** Specifies the Asynchronous Transfer Mode (ATM) service class for the quality-of-service (QoS) contract. Also referred to as ATM service category.

**Usage** Valid values are as follows:

- `cbr` (the default)—Specifies constant bit rate, a service class for connections that depend on precise clocking to ensure undistorted delivery of bits.
- `vbr-rt`—Specifies variable bit rate (VBR)-real time, a service class that handles the packaging of special delay-sensitive applications (such as packet video) that require low cell-delay variation between end points.
- `vbr-nrt`—Specifies VBR-nonreal time, a service class that handles packaging for the transfer of long, bursty data streams over a preestablished ATM connection.
- `ubr`—Specifies unspecified bit rate, a service class that handles bursty LAN traffic, as well as data that accepts delays and cell loss. It is a best-effort service that does not specify bit rates or traffic values, and offers no QoS guarantees.

**Example** `set qos-class = ubr`

**Dependencies** If `encapsulation-protocol` is not set to `atm` or `atm-circuit`, `qos-class` does not apply.

**Location** `ATM-QOS`

### qos-contract

**Description** Specifies the Asynchronous Transfer Mode (ATM) quality-of-service (QoS) contract for the connection.

**Usage** Valid values are as follows:

- `cbr` (the default)—Constant bit rate, for connections that depend on precise clocking to ensure undistorted delivery of bits.
- `real-time-vbr`—Variable bit rate(VBR)-real time, which handles the packaging of special delay-sensitive applications (such as packet video) that require low cell-delay variation between end points.
- `non-real-time-vbr`—VBR-nonreal time, which handles packaging for the transfer of long, bursty data streams over a preestablished ATM connection.
- `abr`—Available bit rate.
- `ubr`—Unspecified bit rate, which handles bursty LAN traffic, as well as data that accepts delays and cell loss. It is a best-effort service that does not specify bit rates or traffic values, and offers no QoS guarantees.

**Example** `set qos-contract = cbr`

**Dependencies** If encapsulation-protocol is not set to atm or atm-circuit, qos-contract does not apply.

**Location** CONNECTION:atm-options  
CONNECTION:atm-connect-options

## qos-interface-group

**Description** Assigns a number to an interface by the administrator. The system matches this number to the interface-group value in a packet-flows profile to classify traffic received on the interface.

**Usage** A number from 0 (the default) to 255, representing a group ID.

**Example** set qos-interface-group = 1

**Location** CONNECTION/":ip-options  
IP-INTERFACE/{ { shelf-1 first-control-module 1 } 0 }

## query-interval

**Description** Specifies the number of seconds between general queries.

**Usage** Specify a number from 0 through 1024. You can increase this value from its default of 125 seconds to reduce the number of IGMP queries sent on the interface.

**Example** set query-interval = 250

**Location** CONNECTION:ip-options:igmp-options

## query-response-interval

**Description** Specifies the maximum response time (in tenths of a second) inserted into general queries.

**Usage** Specify a number from 0 through 1024. You can increase this value from its default of 10 seconds to make IGMP traffic less bursty, because host responses will be spread out over a larger interval.

**Example** set query-response-interval = 20

**Dependencies** The number of seconds of response time (the value of query-response-interval divided by 10) must be less than the query-interval value.

**Location** CONNECTION:ip-options:igmp-options

## queue-depth

**Caution** Specifies the number of packets that can be held for transmission for Simple Network Management Protocol (SNMP) requests. Packets in excess of this number are dropped.

**Usage** Specify a number from 0 to 65535. The default is 0, which specifies that the Stinger unit does not drop packets, no matter how far behind the SNMP subsystem gets. If the queue grows too large in a heavily loaded environment, the system can run out of memory.

**Example** `set queue-depth = 25`

**Dependencies** When setting this value, you are trading memory resources for SNMP retries in the event that the Stinger unit is busy and falls behind in transmitting the SNMP packets.

**Location** `SNMP`

## queue-index

**Description** Specifies the queue of the outgoing trunk port that is associated with the virtual path identifier (VPI) of the path whose traffic is shaped.

**Usage** Specify a number from 0 to 62. A value of zero inactivates the shaper.

**Example** `set queue-index = 5`

**Dependencies** You must specify an additional, separate queue in the `outgoing-queue N` subprofile before this parameter is set.

**Location** `SWITCH-CONFIG:atm-parameters:outgoing-shaper`

## queue-priority

**Description** Priority of the queue for packet flows that match the `packet-classifier` rules in the `flowsubprofile`.

**Usage** Valid values are from 0 to 7, with 0 meaning the lowest and 7 the highest priority. The default value is 0.

**Example** `set queue-priority = 1`

**Location** `PACKET-FLOWS/":flow[1]:scheduling`

## R

### racp-chcs-error-count

**Description** Read-only. Indicates the number of receive ATM cell processor (RACP) correctable header check sequence (CHCS) errors. The RACP delineates ATM cells and filters cells on the basis of their idle status, unassigned status, or HCS errors. It also descrambles the cell payload.

**Usage** The racp-chcs-error-count value is read-only.

**Example** racp-chcs-error-count = 0

**Location** OC3-ATM-STAT

### racp-rx-cell-count

**Description** Read-only. Indicates the receive ATM cell processor (RACP) receive cell count.

**Usage** The racp-rx-cell-count value is read-only.

**Example** racp-rx-cell-count = 0

**Location** OC3-ATM-STAT

**See Also** tacp-tx-cell-count

### racp-uchcs-error-count

**Description** Read-only. Indicates the number of receive ATM cell processor (RACP) uncorrectable header check sequence (UCHCS) errors. The RACP delineates ATM cells and filters cells on the basis of their idle status, unassigned status, or HCS errors. It also descrambles the cell payload.

**Usage** The racp-uchcs-error-count value is read-only.

**Example** racp-uchcs-error-count = 0

**Location** OC3-ATM-STAT

**See Also** racp-chcs-error-count



## rad-id-source-unique

**Description** *Not used.* Specifies whether each RADIUS accounting request should be identified by the user datagram protocol (UDP) source port value, as well as by RADIUS ID, to extend the available number of unique IDs for accounting requests.

RADIUS uses ID values in Request-Response matching. For each unique accounting request (including retries, if a response is not received within the configured timeout period), RADIUS assigns an 8-bit ID value. The assigned value is freed when the request is no longer pending—that is, when RADIUS matches a request with a response, or the request times out.

When the Stinger unit runs at high capacity, RADIUS can run out of unique IDs. By default, when the server reaches its limit of 256 outstanding requests, no unique values are available for the next accounting request. To overcome this limitation, you can specify that each request be identified by the UDP source port as well as by the RADIUS ID value.

## rad-id-space

**Description** *Not used.*

## radius-change-enabled

**Description** Specifies whether the system generates a trap (notification) when a new RADIUS server is being accessed. This trap returns the objectID and IP address of the new server.

**Usage** Valid values are as follows:

- **yes**—Specifies that the system generates a trap when a new RADIUS server is being accessed. This is the default.
- **no**—Specifies that the system does not generate a trap when a new RADIUS server is being accessed.

**Example** `set radius-change-enabled = no`

**Location** `TRAP host-name`

**See Also** `event-overwrite-enabled`

## ra-downshift-int-down

**Description** *Not currently used.* Specifies the number of seconds that the downshift noise margin can be maintained before the line reduces its downstream bit rate.

**Usage** When this parameter becomes available you will be able to specify a value from 1 to 255.

**Example** `set ra-downshift-int-down=15`

**Location** `AL-DMT:margin-config`

**See Also** `ra-downshift-int-up`

## ra-downshift-int-up

**Description** *Not currently used.* Specifies the number of seconds that the downshift noise margin can be maintained before the line reduces its upstream bit rate.

**Usage** When this parameter becomes available you will be able to specify a value from 1 to 255.

**Example** set ra-downshift-int-up = 15

**Location** AL-DMT:margin-config

**See Also** rarp-enabled

## ra-downshift-margin-down

**Description** *Not currently used.* Specifies the downstream noise margin relative to zero decibels (dB). If the noise level remains at this level for more than the specified time interval, the line reduces its downstream bit rate.

**Usage** When this parameter becomes available you will be able to specify a value from 1 to 31 dB.

**Example** set ra-downshift-margin-down = 15

**Location** AL-DMT:margin-config

**See Also** ra-downshift-margin-up

## ra-downshift-margin-up

**Description** *Not currently used.* Specifies the upstream noise margin relative to 0 dB. If the noise level remains at this level for more than the specified time interval, the line reduces its upstream bit rate.

**Usage** When this parameter becomes available you will be able to specify a value from 1 to 31 dB.

**Example** ra-downshift-margin-up = 15

**Location** AL-DMT:margin-config

**See Also** ra-downshift-margin-down

## rad-serv-enable

**Description** Specifies whether or not the on-board RADIUS server is enabled.

**Usage** Valid values are as follows:

- **yes**—Specifies that the RADIUS server is enabled.
- **no**—Specifies that the RADIUS server is not enabled. This is the default.

**Example** `set rad-serv-enable = yes`

**Location** EXTERNAL-AUTH

## rarp-enabled

**Description** Enables or disables obtaining the system's IP addresses from a Reverse Address Resolution Protocol (RARP) server.

**Usage** Specify yes or no. The default is no.

- **yes**—Enable the Stinger unit to use RARP to obtain its IP address from a RARP server.
- **no**—Disable the Stinger unit's ability to use RARP.

**Example** `set rarp-enabled = yes`

**Location** IP-GLOBAL

## rate-adapt-mode-down

**Description** Specifies the rate-adaptive mode for downstream training.

**Usage** Specify one of the following values:

- **automatic-at-startup** (the default)—Specifies that the downstream rate is selected at startup. If you accept the **automatic-at-startup** default, the customer premises equipment (CPE) initializes at a minimum specified bit rate and target noise margin.

If the CPE fails to achieve the minimum bit rate in either direction, it cannot initialize, and it sends a message that the requested bit rate was too high. If the CPE can support a higher bit rate than the specified minimum, it can train up to a higher rate within the acceptable noise margin. Each direction can specify a different minimum and maximum bit rate for using the fast or interleaved ADSL channel.

- **operator-controlled**—Specifies that the line trains downstream using a constant planned bit rate. The CPE must initialize at and maintain a specific bit rate with an acceptable target noise margin.

If the CPE fails to achieve the planned bit rate in either direction, it fails to initialize. The CPE does not use a higher bit rate, even if it can support one.

- **dynamic**—*Not currently used.*

**Example** `set rate-adapt-mode-down = operator-controlled`

**Dependencies** By default, the `rate-adapt-mode-up` and `rate-adapt-mode-down` parameters in the `al-dmt:line-config` subprofile are set to `automatic-at-startup`. To change the setting to `operator` for *both* the `rate-adapt-mode-up` and `rate-adapt-mode-down` parameters, you need only configure the `rate-adapt-mode-up` parameter.

**Location** `AL-DMT:line-config`

**See Also** `rate-adapt-mode-up`

## rate-adapt-mode-up

**Description** Specifies the rate-adaptive mode for upstream training.

**Usage** Specify one of the following values:

- `automatic-at-startup`—Specifies that the upstream rate is selected at startup. If you accept the `automatic-at-startup` default, the customer premises equipment (CPE) initializes at a minimum specified bit rate and target noise margin.

If the CPE fails to achieve the minimum bit rate in either direction, it cannot initialize, and sends a message that the requested bit rate was too high. If the CPE can support a higher bit rate than the specified minimum, it can train up to a higher rate within the acceptable noise margin. Each direction can specify a different minimum and maximum bit rate for using the fast or interleaved ADSL channel. This is the default.

- `operator-controlled`—Specifies that the line trains upstream using a constant planned bit rate. The CPE must initialize at and maintain a specific bit rate with an acceptable target noise margin.

If the CPE fails to achieve the planned bit rate in either direction, it fails to initialize. The CPE does not use a higher bit rate, even if it can support one.

- `dynamic`—*Not currently used.*

**Example** `set rate-adapt-mode-down = operator-controlled`

**Dependencies** By default, the `rate-adapt-mode-up` and `rate-adapt-mode-down` parameters in the `al-dmt:line-config` subprofile are set to `automatic-at-startup`. To change the setting to `operator` for *both* the `rate-adapt-mode-up` and `rate-adapt-mode-down` parameters, you need only configure the `rate-adapt-mode-up` parameter.

**Location** `AL-DMT:line-config`

**See Also** `rate-adapt-mode-down`

## rate-adapt-ratio-down

**Description** *Not currently used.* Specifies the ratio for distributing excess downstream bit rate among the fast and interleaved channels when dual latency is supported.

**Usage** Specify a percentage from 0 to 100 percent. 100 percent is the default.

**Example** `rate-adapt-ratio-down = 100`

**Dependencies** This parameter is valid only when `rate-adapt-mode` is set to `automatic_at_startup` or `dynamic`.

**Location** `AL-DMT:line-config`

## rate-adapt-ratio-up

**Description** *Not currently used.* Specifies the ratio for distributing excess upstream bit rate among the fast and interleaved channels when dual latency is supported.

**Usage** Specify a percentage from 0 to 100 percent. 100 percent is the default.

**Example** `rate-adapt-ratio-up = 100`

**Dependencies** This parameter is valid only when `rate-adapt-mode` is set to `automatic_at_startup` or `dynamic`.

**Location** `AL-DMT:line-config`

## rate-mode

**Description** Specifies whether the HDSL2 or SHDSL line rate is fixed or adaptive (also called automatic).

**Usage** Specify one of the following values:

- `fixed`—The modem tries to establish a connection only at a rate specified by the setting of the `max-rate` parameter. Noise margin settings of the `margin` and `snext-margin` parameters are not considered.
- `auto`—After an adaptive probe establishes the line characteristics, the modem tries to establish a connection at the maximum rate possible between the `max-rate` and `min-rate` settings that satisfies the settings of the `margin` and `snext-margin` parameters. This is the default setting.

**Dependencies** This parameter applies only if the `interface-type` parameter is set to `g-shdsl`.

**Example** `set rate-mode = fixed`

**Location** `HDSL2:line-config`  
`SHDSL:line-config`

## ratio-centralized-detection

**Description** *For internal use only.*

## ra-upshift-int-down

**Description** *Not currently used.* Specifies the number of seconds that the upshift noise margin can be maintained before the line increases its downstream bit rate.

**Usage** Specify a value from 1 to 255.

**Example** `set ra-upshift-int-down = 15`

**Location** AL-DMT:margin-config

**See Also** ra-upshift-int-up

## ra-upshift-int-up

**Description** *Not currently used.* Specifies the number of seconds that the upshift noise margin can be maintained before the line increases its upstream bit rate.

**Usage** Specify a value from 1 to 255.

**Example** `set ra-upshift-int-up = 15`

**Location** AL-DMT:margin-config

**See Also** ra-upshift-int-down

## ra-upshift-margin-down

**Description** *Not currently used.* Specifies the downstream noise margin relative to zero decibels (dB). If the noise level remains at this level for more than the specified time interval, the line increases its downstream bit rate.

**Usage** Specify a value from 1dB to 31dB.

**Example** `set ra-upshift-margin-down = 15`

**Location** AL-DMT:margin-config

**See Also** ra-upshift-margin-up

## ra-upshift-margin-up

**Description** *Not currently used.* Specifies the upstream noise margin relative to 0 dB. If the noise level remains at this level for more than the specified time interval, the line increases its upstream bit rate.

**Usage** Specify a value from 1dB to 31dB.

**Example** `set ra-upshift-margin-up = 15`

**Location** AL-DMT:margin-config

**See Also** ra-upshift-margin-down

## rcv-tone-frequency

**Description** Read-only. Reports the receive tone frequency in herz during a copper loop test (CLT) module test.

**Usage** This is a read-only value.

**Example** `rcv-tone-frequency = 0`

**Location** CLT-RESULT

**See Also** `rcv-tone-level`

## rcv-tone-level

**Description** Read-only. Reports the receive tone level in hundredths (0.01) dBm during a copper loop test (CLT) module test.

**Usage** This is a read-only value.

**Example** `rcv-tone-level = 0`

**Location** CLT-RESULT

**See Also** `rcv-tone-frequency`

## reach-type

**Description** Identifies the type of transceiver on the trunk module.

**Usage** For the `transceiver-info` profile, this parameter has the following read-only values which indicate the module type in the applicable slot:

- `short-reach`—Indicates a short reach module.
- `intermediate-reach`—Indicates an intermediate reach module.
- `long-reach`—Indicates a long reach module.
- `reach-none` (the default)—Indicates no module is detected.

**Example** `reach-type = long-reach`

**Location** TRUNK-DAUGHTER-DEV:transceiver-info

## read-access-hosts [n]

**Description** An array containing up to five IP addresses of Simple Network Management Protocol (SNMP) managers that have read permission. If `enforce-address-security` is set to `yes`, the Stinger unit responds to SNMP Get and Get-Next commands from only the SNMP managers you specify in the array.

**Usage** For each element in the array, you can specify an IP address in dotted decimal notation.

**Example** `set read-access-hosts 1 = 10.2.3.4/24`

**Dependencies** You must set `enforce-address-security` to `yes` for the address to have any effect.

**Location** `SNMP`

## `read-community`

**Description** Specifies a Simple Network Management Protocol (SNMP) community name. An SNMP manager must send the correct community name to access the SNMP Get and Get-Next commands.

**Usage** Specify the community name. You can enter up to 32 characters. The default is `public`. Asterisks are displayed in place of the name.

**Example** `set read-community = mycomm`

**Location** `SNMP`

## `read-view-name`

**Description** Specifies the name of a view for read access in a view-based access control model (VACM).

**Usage** Specify a name of up to 32 characters. If a request that matches the access-properties specified in this profile uses this name, read access is granted. The default name is a null string.

**Example** `set read-view-name = elsinore`

**Location** `VACM-ACCESS`

**See Also** `access-properties`

## `read-write-access`

**Description** Enables or disables read-write access to the unit's MIBs for this user.

**Usage** With the default value `no`, the user has read access only, which enables viewing but not modification of the MIBs. Specify `yes` or `no`

- `yes`—Enables read/write access.
- `no`—Enables read access only. This is the default.

**Example** `read-write-access = no`

**Location** `SNMPv3-USM-USER`



## read-write-community

**Description** Specifies a read/write Simple Network Management Protocol (SNMP) community name. An SNMP manager must send the correct community name to access the SNMP Get, Get-Next, and Set commands.

**Usage** Specify the community name. You can enter up to 32 characters. The default is `write`.

**Example** `set read-write-community = secret`

**Location** `SNMP`

## read-write-enabled

**Description** Specifies whether the read/write community can be accessed by means of SNMP.

**Usage** Valid values are as follows:

- `yes`—Specifies that the read/write community can be accessed by means of SNMP. This is the default.
- `no`—Specifies that the read/write community cannot be accessed by means of SNMP.

**Example** `set read-write-enabled = yes`

**Location** `SNMP`

**See Also** `read-write-access`

## real-time-vbr

**Description** Enables or disables real-time variable bit rate (VBR) traffic in this queue.

**Usage** Valid values are as follows:

- `yes`—This queue supports ATM real-time VBR traffic.
- `no` (the default)—The queue does not support real-time VBR traffic. This is the default.

For each queue, one or more ATM services categories can be set to `yes`. The `real-time-vbr` parameter must be set to `yes` for at least one and no more than two of the active queues assigned to a LIM, control module, or trunk.

**Location** `SWITCH-CONFIG:atm-parameters:outgoing-queue`

## receive-auth-mode

**Description** Specifies the authentication protocol to use for incoming PPP session requests. RADIUS is required for dynamic password using token cards.

**Usage** Specify one of the following values:

- `no-ppp-auth` (the default)—no authentication is required.
- `pap-ppp-auth`—The connection must use Password Authentication Protocol (PAP). The remote end sends its password in the clear. The password is not encrypted.
- `chap-ppp-auth`—The connection must use Challenge Handshake Authentication Protocol (CHAP). The remote end does not send its password in the clear. An MD5 digest calculated from the password and a random challenge are sent instead.
- `any-ppp-auth`—The connection must use PAP or CHAP or MS-CHAP (Microsoft's extension of CHAP).
- `des-pap-ppp-auth`—The connection must use PAP with dynamic passwords.
- `token-pap-ppp-auth`—The connection must use PAP with dynamic passwords. The system uses one-time Data Encryption Standard (DES) password encryption and sends a challenge in the token.
- `token-chap-ppp-auth`—The connection must use `pap-token` for the first call of a multichannel session, and CHAP for additional channels.
- `cache-token-ppp-auth`—The connection must use CHAP with dynamic passwords. The system uses CHAP with challenges, but caches token responses and uses them for authenticating additional channels.
- `ms-chap-ppp-auth`—The connection must use MS-CHAP, designed mostly for Windows NT or LAN Manager platforms.
- `pap-preferred`—The connection must use PAP or CHAP or MS-CHAP, but PAP is attempted first. If PAP is rejected by the client, then either CHAP or MS-CHAP is used.

**Example** `set receive-auth-mode = any-ppp-auth`

**Dependencies** When `receive-auth-mode` is set to any value other than `no-ppp-auth`, all connection or RADIUS profiles that specify PPP encapsulation must also specify a password. RADIUS is required for dynamic passwords using token cards.

**Location** `ANSWER-DEFAULTS:ppp-answer`

**See Also** `ppp-answer`

## received-rs-blocks

**Description** Read-only. Indicates the number of received Reed-Solomon blocks. Indicates the number of received ADSL superframes (blocks) for Centillium-based line-interface modules (LIMs) and Stinger MRT units.

**Usage** The `received-rs-blocks` parameter is a read-only display for checking operations.

**Example** received-rs-blcks = 104073

**Location** AL-DMT-STAT:physical-statistic

**See Also** incoming-cells, transmitted-rs-blocks

## receive-equalization

**Description** Enables or disables receive equalization. Receive equalization is needed if the cable length is more than 450 feet (157m).

**Usage** Valid values are as follows:

- no (the default)—Receive equalization is not enabled.
- yes—Receive equalization is enabled.

**Example** set receive-equalization = yes

**Location** DS3-ATM:line-config

## receive-sdu-size

**Description** Size of the receive service data unit (SDU) in octets.

**Usage** Specify a value between 1 and 2000 octets. One octet is the default value.

**Example** set receive-sdu-size = 128

**Location** CONNECTION:atm-aal-options

## rec-link-cond-time

**Description** *Not currently used.* Specifies the amount of time that must elapse before link conditioning timeout takes place during link recovery,

**Usage** Specify a number from 0 through 2147483647.

**Example** set rec-link-cond-time = 10

**Location** DS1-ATM:line-config:ima-option-config:rxlink-config

## recv-channel-mismatch-count

**Description** Read-only. Indicates the number of channel-mismatch events received in the automatic protection switching (APS) system.

**Usage** The valid range for this read-only parameter is from 0 through 2147483647. The default value is 0 (zero).

**Example** recv-channel-mismatch-count = 49

**Location** APS-STAT

## recv-fepl-count

**Description** Read-only. Indicates the number of far end protection line (FEPL) events received in the automatic protection switching (APS) system.

**Usage** The valid range for this read-only parameter is from 0 through 2147483647. The default value is 0 (zero).

**Example** `recv-fepl-count = 15`

**Location** APS-STAT

## recv-mode-mismatch-count

**Description** Read-only. Indicates the number of mode-mismatch events received in the automatic protection switching (APS) system.

**Usage** The valid range for this read-only parameter is from 0 through 2147483647. The default value is 0 (zero).

**Example** `recv-mode-mismatch-count = 0`

**Location** APS-STAT

## recv-password

**Description** Specifies the password that the Stinger unit must receive from the device initiating the PPP session request.

**Usage** Specify a text string of up to 20 characters. The password is case sensitive. If the Stinger unit does not require a password from the remote end, accept the default of null.

**Example** `set recv-password = remote`

**Dependencies** This setting does not apply if `receive-auth-mode` is set to `no-ppp-auth`. If `receive-auth-mode` is set to any other value, you must specify a password or the incoming request will fail authentication.

**Location** CONNECTION:ppp-options

## recv-psbf-count

**Description** Read-only. Indicates the number of protection switching byte failure (PSBF) events received in the automatic protection switching (APS) system.

**Usage** The valid range for this read-only parameter is from 0 through 2147483647. The default value is 0 (zero).

**Example** `recv-psbf-count = 42`

**Location** APS-STAT

## redirect-address

**Description** Specifies an IP address to which matching packets are redirected. Port redirection enables you to redirect any TCP or UDP packet to a specified server on the basis of its protocol and port information. For example, you can redirect HTTP traffic to a Web cache server on a local network.

**Usage** Specify an IP address. Packets that match the protocol setting received on the port specified in the port-number parameter are redirected to the specified address.

**Example** `set redirect-address = 3.3.3.3/28`

**Location** CONNECTION:port-redirect-options

**See Also** port-redirect-options

## reelect-time

**Description** Specifies the number of seconds that the node waits after losing connectivity to the current peer group leader before restarting the process of electing a new peer group leader.

**Usage** Specify the number of seconds to wait. The default value is 15 seconds.

**Example** `set reelect-time = 15`

**Location** PNNI-NODE-CONFIG[n]:node-pgl

## regional

**Description** *Not currently used.* Specifies a regional number from 0 to 104 representing the highest level of the PNNI hierarchy that lies within the regional scope. The default value is 32.

## relative-delay

**Description** Read-only. Indicates the latest measured delay on this link relative to the link, in the same inverse multiplexing over ATM (IMA) group, with the least delay.

**Usage** The valid range for this read-only value is from 0 through 2147483647.

**Example** `relative-delay = 0`

**Location** DS1-ATM-STAT:ima-link-status

## remote-address

**Description** Specifies an IP address of the remote device, which can include a subnet specification. If the address does not include a subnet mask, the router assumes the default subnet mask based on address class.

The system uses this value to match the address presented by an incoming IP connection.

**Usage** Specify an IP address. The default is the null address (0.0.0.0/0).

**Example** `set remote-address = 1.2.3.4/32`

**Location** CONNECTION:ip-options  
CONNECTION:bir-options:multiple-ip-address:ip-address-option[n]

## remote-configuration

**Description** *Not used.*

## remote-shelf-enabled

**Description** Specifies whether the remote shelves sensors trap (notification) is enabled.

**Usage** Valid values are as follows:

- yes (the default)—Specifies that the remote shelves sensors trap is enabled.
- no—Specifies that the remote shelves sensors trap is disabled.

**Example** `set remote-shelf-enabled = no`



**Note** To enable the system to send traps related to sensors on remote shelves, the following parameters must be set to yes (their default value):

```
[in TRAP/""]
remote-shelf-enabled = yes
watchdog-warning-enabled = yes
```

**Location** TRAP

**See Also** watchdog-warning-enabled

## remote-shelf-id

**Description** The shelf ID of the remote shelf. This value is set by the system when it detects the remote shelf across the cascade port.

**Usage** The remote-shelf-id value is read-only. The value is the shelf identification number preceded by shelf- of the remote shelf.

**Example** `remote-shelf-id = shelf-3`

**Location** REMOTE-SHELF-CONFIG  
REMOTE-SHELF-STAT

## remote-shelf-oper-state

**Description** The operational state of the remote shelf.

**Usage** This parameter is read-only. The following list summarizes possible values:

|                              |                                                                                       |
|------------------------------|---------------------------------------------------------------------------------------|
| remote-shelf-oper-state-down | The remote shelf is down, a non-operational state.                                    |
| remote-shelf-oper-state-up   | The remote shelf is operating normally.                                               |
| remote-shelf-link-failed     | Link failure was detected on the link connecting this remote shelf to the main shelf. |
| remote-shelf-discovering     | Remote shelf discovery in progress.                                                   |
| remote-shelf-discovery-up    | Remote shelf discovered.                                                              |
| remote-shelf-ms-link-down    | The logical control channel is down between this remote shelf and the host.           |

**Example** remote-shelf-oper-state = remote-shelf-oper-state-up

**Location** REMOTE-SHELF-STAT

## remote-shelf-type

**Description** Displays the type of remote shelf.

**Usage** The remote-shelf-type value is read-only. It must always display stngr-cascaded-mrt in Stinger MRT multishelf systems.

**Example** remote-shelf-type = stngr-cascaded-mrt

**Location** REMOTE-SHELF-CONFIG

## repeat-ustat

**Description** Enables or disables sending two USTAT messages each time a USTAT message is required.

**Usage** This parameter is disabled by default.

**Example** repeat-ustat = no

**Location** ATM-IF-SIG-PARAMS:qsaal-options

## reqd-state

**Description** The required operational state of the module in the slot. Changing this value initiates a change to the required state.

**Usage** Specify one of the following values:

- reqd-state-up—The module is required to be in a normal operating state.
- reqd-state-down—The module is required to be in the down state.
- reqd-state-maint—The module is required to be in the maintenance state.

**Example** `set reqd-state = reqd-state-down`

**Location** `SLOT-ADMIN`

## `restart-after-trap`

**Description** Specifies whether you want to continue testing after a trap (notification) is generated.

**Usage** Specify one of the following settings:

- `yes`—Specifies that testing continues after a trap is generated.
- `no` (the default)—Specifies that testing does not continue after a trap is generated.

**Example** `set restart-after-trap = yes`

**Dependencies** This parameter has no effect in the case of profiles created for multiple testing. In that case, the test is always restarted.

**Location** `ATM-OAM:loopback-config`

## `restrict-redundancy-enabled`

**Description** *Not used.*

**Location** `BASE`

## `retransmit-interval`

**Description** Specifies the number of seconds between retransmissions of Open Shortest Path First (OSPF) protocol packets. OSPF uses the `retransmit-interval` value for link state advertisement (LSA) transmissions, and for retransmitting Database Description and Link State Request packets.

**Usage** Specify a number greater than zero. The default is 5.

**Example** `set retransmit-interval = 15`

**Location** `IP-INTERFACE:ospf`  
`CONNECTION:ip-options:ospf-options`

## `retry-count`

**Description** Specifies the number of times the system retransmits control packets in the attempt to establish or reestablish a tunnel. Any change you make to this value takes effect when the previous timer expires.

**Usage** Specify a number from 1 to 10. The default is 6.



**Example** `set retry-count = 10`

**Dependencies** This counter works with the `first-retry-timer` parameter in establishing and maintaining tunnel sessions.

**Location** `L2-TUNNEL-GLOBAL:l2tp-config`

## retry-limit

**Description** Specifies the maximum number of failed attempts to establish an Ascend Tunnel Management Protocol (ATMP) tunnel to the primary Home Agent before switching to the secondary Home Agent.

Together with the `retry-timeout` setting, this parameter specifies how many tunnel RegisterRequest and DeregisterRequest messages are sent and the number of seconds between each message. Both parameters have default settings that are appropriate for most sites.

**Usage** Specify a number, from 1 through 100. The default is 10.

**Example** `set retry-limit = 25`

**Location** `ATMP`

## retry-time

**Description** *Not currently used.* Specifies the number of seconds the node waits before attempting to reestablish a switched virtual channel connection (SVCC) where that RCC appears to be still necessary and viable but that has unexpectedly terminated.

**Location** `PNNI-NODE-CONFIG:node-svcc-rcc`

## retry-timeout

**Description** Specifies the number of seconds between retries to establish an Ascend Tunnel Management Protocol (ATMP) tunnel.

Together with the `retry-limit` setting, this parameter specifies how many tunnel RegisterRequest and DeregisterRequest messages are sent and the number of seconds between each message. Both parameters have default settings that are appropriate for most sites.

**Usage** Specify a number of seconds, from 1 through 120. The default is 3.

**Example** `set retry-timeout = 5`

**Location** `ATMP`

## reverse-path-check

**Description** Enables or disables level 2 antispoofing protection.

**Usage** Valid values are as follows:

- **yes**—Specifies that the system checks the routing table to verify that it can reach the packet's source address across the same interface on which it received the packet, and drops nonmatching packets.
- **no** (the default)—Specifies that antispoofing for the session is disabled.

**Example** `set reverse-path-check = yes`

**Dependencies** This setting and the `source-ip-check` setting are mutually exclusive. Only one of these fields can be enabled in a profile.

**Location** CONNECTION:ip-options

## revertive-mode

**Description** Specifies or indicates, according to the profile, whether the connection returns to the working line from the protection line once the working line has recovered in an automatic protection switching (APS) system.

**Usage** Valid values are as follows:

- **revertive** (the default)—The connection reverts to the working line once it is restored and the waiting time to revert has elapsed. The default is revertive.
- **non-revertive**—The connection does not revert to the working line once it is restored.

**Example** `set revertive-mode = non-revertive`

**Location** APS-CONFIG  
APS-STAT

## rexmit-delay

**Description** Specifies the number of seconds between retransmissions of Open Shortest Path First (OSPF) protocol packets between virtual links.

OSPF uses the `xmit-delay` value for link state advertisement (LSA) transmissions, and for retransmitting Database Description and Link State Request packets.

**Usage** Specify a number greater than zero. The default is 1.

**Example** `set rexmit-delay = 15`

**Location** OSPF-VIRTUAL-LINK

## ringer

**Description** Indicates the results of a copper loop test (CLT) module ringer detection test.

**Usage** Read-only value with one of the following values:

- no—Ringer is not detected.
- yes—Ringer is detected.

**Example** ringer = yes

**Location** CLT-RESULT

## rip

**Description** Enables or disables Routing Information Protocol (RIP) updates on the interface.

**Usage** Specify one of the following values:

- routing-off—Do not send routing updates, and ignore any routing updates received for the connection. This is the default.
- routing-send-only—Send RIP-v1 routing updates, but ignore any received for the connection.
- routing-recv-only—Do not send RIP-v1 routing updates, but accept any routing updates received for the connection.
- routing-send-and-recv—Send RIP-v1 routing updates and accept any received for the connection.
- routing-send-only-v2—Send RIP-v2 routing updates, but ignore any received for the connection.
- routing-recv-only-v2—Do not send RIP-v2 routing updates, but accept any routing updates received for the connection.
- routing-send-and-recv-v2—Send RIP-v2 routing updates and accept any received for the connection.

**Example** set rip = routing-send-only-v2

**Location** CONNECTION:ip-options  
IP-INTERFACE

**See Also** ip-interface, ip-options

## rip2-use-multicast

**Description** Enables or disables use of the multicast address (224.0.0.9) rather than the broadcast address for RIP updates. By default, RIP updates use the multicast address.

**Usage** Valid values are as follows:

- **yes** (the default)—Enables RIP-v2 to use the multicast address (224.0.0.9) instead of the broadcast address for its updates.
- **no**—Disables the use of the multicast address for RIP updates. Use this setting if you must use the broadcast address for backward compatibility with other systems.

**Example** `set rip2-use-multicast = yes`

**Dependencies** This setting does not apply when `rip-mode` specifies RIP version 1.

**Location** IP-INTERFACE

## rip-mode

**Description** Specifies whether the interface should run Routing Information Protocol (RIP) version 1 or RIP version 2, and whether it should send updates, receive them, or both.

The Internet Engineering Task Force (IETF) has voted to move RIP-v1 into the *historic* category, and its use is no longer recommended. You should upgrade all routers and hosts to RIP-v2. If you must maintain RIP-v1, Lucent Technologies recommends that you create a separate subnet, and place all RIP-v1 routers and hosts on that subnet.

**Usage** Valid values are as follows:

| Value                                  | Specifies that the Stinger unit                                                                       |
|----------------------------------------|-------------------------------------------------------------------------------------------------------|
| <code>routing-off</code> (the default) | Does not send routing updates, and ignores any routing updates it receives for the connection.        |
| <code>routing-send-only</code>         | Sends RIP-v1 routing updates, but ignores any it receives for the connection.                         |
| <code>routing-recv-only</code>         | Does not send RIP-v1 routing updates, but accepts any routing updates it receives for the connection. |
| <code>routing-send-and-recv</code>     | Sends RIP-v1 routing updates and accepts any it receives for the connection.                          |
| <code>routing-send-only-v2</code>      | Sends RIP-v2 routing updates, but ignores any it receives for the connection.                         |
| <code>routing-recv-only-v2</code>      | Does not send RIP-v2 routing updates, but accepts any routing updates it receives for the connection. |
| <code>routing-send-and-recv-v2</code>  | Sends RIP-v2 routing updates and accepts any it receives for the connection.                          |

**Example** `set rip-mode = routing-send-only-v2`

**Location** IP-INTERFACE

## rip-policy

**Description** Specifies the policy for sending update packets that include routes received on the same interface when the system supports RIP-v1.

**Usage** Valid values are as follows:

- `poison-rvrs` (the default)—Propagate routes back to the subnet from which they were received, but with a metric of 16 (infinite metric).
- `split-horzn`—Do not propagate routes back to the subnet from which they were received.

**Example** `set rip-policy = split-horzn`

**Dependencies** This setting applies only when the system supports RIP-v1. In a `vrouter` profile, default settings related to RIP are recommended for most sites.

**Location** IP-GLOBAL  
VROUTER

**See Also** `ip-global`, `vrouter`

## rip-pref

**Description** Specifies the default preference for routes that the system learns from RIP. When choosing the routes to put in the routing table, the router first compares their preference values, preferring the lowest number. If the preference values are equal, the router compares the metric values, using the route with the lowest metric.

**Usage** Specify a number from 0 to 255. A value of 255 prevents the use of the route. Following are the default preferences for different types of routes:

- 0 (zero)—Connected routes
- 10—OSPF routes
- 30—Routes learned from ICMP redirects
- 100—Routes learned from RIP
- 100—Static routes
- 100—ATMP routes

**Example** `set rip-pref = 50`

**Location** IP-GLOBAL

## rip-queue-depth

**Description** Specifies the maximum number of RIP packets to be held for processing. To prevent delays in routing, UDP processing runs at a lower priority than the processing of routed packets. On a system busily routing packets, this behavior can cause a backlog of UDP packets to build up. This parameter specifies how many RIP update packets to queue before the system begins dropping RIP packets.

**Usage** Specify the maximum number of RIP update packets to queue. Valid values are from 0 through 1024. The default value is 50.

- The value of 0 means that the queue is unlimited.
- If you specify a nonzero queue depth, the Stinger unit is more likely to drop UDP packets when it is busy routing packets, but time-sensitive routed packets are less likely to be delayed and system memory is used more efficiently.

**Example** `set rip-queue-depth = 128`

**Location** IP-GLOBAL

## rip-tag

**Description** Specifies a tag to associate with RIP routes. A tag is a 32-bit hexadecimal number.

**Usage** Specify a 32-bit hexadecimal number. The default is c8:00:00:00.

**Example** `set rip-tag = cf000000`

**Location** IP-GLOBAL

## rip-trigger

**Description** Enables or disables RIP triggering. RIP triggering enables the router or virtual router to tag routes that have been updated in the routing table and send updates that include only the changed routes.

Changes occur when a call arrives or disconnects, RIP learns a route from another router, or the administrator modifies a route-related profile. The router broadcasts updates 5 to 8 seconds after the first change in the routing table is detected. The delay helps to prevent constant updates during peak traffic conditions. The result is reduced processing overhead for both the router and its neighbors.

**Usage** Valid values are as follows:

- `yes` (the default)—Tag changes to the routing table and include only the tagged routes in the next RIP update, 5 to 8 seconds after the first change in the table is detected.
- `no`—Send full table updates every 20 to 40 seconds. To prevent RIP routers on a network from synchronizing and sending large updates in unison, the full table update is no longer broadcast at fixed 30-second intervals.

**Example** `set rip-trigger = yes`

**Dependencies** In a vrouter profile, default settings related to RIP are recommended for most sites.

**Location** IP-GLOBAL  
VROUTER

## rlogin

**Description** *Not used.*

## rlop-bip-error-count

**Description** Read-only. Indicates the number of Receive Line Overhead Processor (RLOP) Bit Interleaved Parity (BIP-8) errors. The RLOP is responsible for line-level alarms and performance monitoring.

**Usage** The rlop-bip-error-count value is read-only.

**Example** `rlop-bip-error-count = 0`

**Location** OC3-ATM-STAT

## rlop-feb-error-count

**Description** Read-only. Indicates the number of Receive Line Overhead Processor (RLOP) far-end block errors (FEBEs).

**Usage** The rlop-febe-error-count value is read-only.

**Example** `rlop-febe-error-count = 0`

**Location** OC3-ATM-STAT

## robust-count

**Description** A threshold of packet losses up to which the multicast subsystem will remain robust.

**Usage** Specify a number from 2 through 2. If the interface is expected to have a high rate of packet loss, increase this value. IGMP is robust to this value -1. It cannot be set to zero and should not be set to 1. The default is 2.

**Example** `set robust-count = 5`

**Location** CONNECTION:ip-options:igmp-options

## root

**Description** Specifies the name of the connection profile to be intercepted (the root profile).

**Usage** Specify a name. The default is null.

**Example** `set root = myconnection`

**Dependencies** Consider the following:

- When you write the leaf profile with the name of a valid connection profile in the atm-options subprofile, the system creates a unidirectional connection from the VCC defined in the atm-options subprofile of the specified root profile to the VCC (the nailed-group, vpi, and vci values) defined in the atm-options subprofile of the leaf profile. Then the system begins transmitting the intercepted traffic to the leaf end point.
- When you write the leaf profile with the name of a valid connection profile in the atm-connect-options subprofile, the system creates a unidirectional connection from the VCC defined in the atm-connect-options subprofile of the specified root profile to the VCC defined in the atm-connect-options subprofile of the leaf profile. Then the system begins transmitting the intercepted traffic to the leaf end point.
- The system always uses the highest-priority queue for outbound intercepted traffic. Therefore, in a leaf connection profile, the following settings are ignored:  
`[in CONNECTION/":atm-qos-options]`  
`usr-up-stream-contract = default`  
`usr-dn-stream-contract = default`

**Location** CONNECTION:atm-connect-options  
CONNECTION:atm-options

## route-address

**Description** Specifies an IP address. After applying the value specified by route-mask parameter, the system compares the result to routes in a RIP packet. If it finds a route with a matching destination, it takes the action specified in the route filter.

**Usage** Specify an IP address. The default is 0.0.0.0, which matches all addresses.

**Example** `set route-address = 3.3.3.3`

**Dependencies** This setting applies only if the type parameter in the input-filter or output-filter subprofile is set to route-filter.

**Location** FILTER:input-filters[n]:route-filter  
FILTER:output-filters[n]:route-filter



## route-filter

**Description** Specifies the name of a filter profile that defines a route filter. The specified route filter will be applied to the interface.

**Usage** Specify the filter name. The default is null, which indicates no filter.

**Example** `set route-filter = route-test`

**Location** CONNECTION:ip-options  
IP-INTERFACE

## route-id

**Description** Specifies the current route ID of a Stinger unit.

**Usage** The route-id setting is a complex field that consists of one component: id.

**Example** `set route-id id = 140`

**Location** DEVICE-STATE

## route-mask

**Description** Specifies a mask that the system applies to the value specified by route-address parameter before comparing the resulting value to routes in a RIP update packet.

You can use this value to hide the host portion of an address, or its host and subnet portion. After translating the mask and address into binary format, the system applies the mask to the address by performing a logical AND operation. The mask hides the portion of the address that appears behind each binary 0 (zero) in the mask.

**Usage** Specify a mask in decimal notation.

- The default is 0.0.0.0, which masks all bits.
- A mask of all ones (255.255.255.255) masks no bits, so the specified route-address value must exactly match a route in a RIP update packet for the comparison to succeed.

**Example** `set route-mask = 255.255.255.255`

**Dependencies** This setting applies only if the type parameter in the input-filter or output-filter subprofile is set to route-filter.

**Location** FILTER:input-filters[n]:route-filter  
FILTER:output-filters[n]:route-filter

## route-port

**Description** *Not used.*

## router-id

**Description** Specifies the router IP address.

**Usage** Specify the IP address including the netmask field if applicable.

**Example** `set router-id = 192.207.23.13`

**Location** IP-GLOBAL

**See Also** `ignore-icmp-redirects`

## route-tns-id

**Description** Specifies the value of the transit network identifier.

**Usage** Specify a string to identify the transit network.

**Example** `set route-tns-id = mixxx0`

**Location** PNNI-ROUTE-TNS:tns-index

## route-tns-index

**Description** Specifies an index that distinguishes between multiple listings of connectivity to a given transit network from the local node.

**Usage** Only the number 1 is currently supported.

**Example** `set route-tns-index = 1`

**Location** PNNI-ROUTE-TNS:tns-index

## route-tns-plan

**Description** Specifies a network identification plan according to which network identification has been assigned.

**Usage** Valid values are as follows:

- `carrier-ident-code`
- `other`—This is the default.

**Example** `set route-tns-plan = other`

**Location** PNNI-ROUTE-TNS:tns-index

## route-tns-type

**Description** Specifies the type of network identification used for this transit network.

**Usage** Valid values are as follows:

- other—Unspecified. This is the default.
- reject—A route that discards traffic
- internal—Directly attached to the logical node advertising the address
- exterior—Reachable through the PNNI routing domain, but not located in the PNNI routing domain.

**Example** set route-tns-type = other

**Location** PNNI-ROUTE-TNS:tns-index

## routing-metric

**Description** Specifies a RIP-style metric for the route. RIP is a distance-vector protocol that uses hop count as its metric. Among routes with the same destination address and equal preference values, a higher metric means that the system is less likely to choose the route.

**Usage** Specify a number from 1 to 15. The default value is 1.

**Example** set routing-metric = 5

**Location** ANSWER-DEFAULTS:ip-answer  
CONNECTION:ip-options

## routing-protocols-disabled

**Description** *Not used.*

**Location** BASE

## rp-address

**Description** IP address of the rendezvous point (RP). The address must be reachable throughout the domain.

**Usage** Specify an IP address in dotted decimal notation.

**Example** set rp-address = 1.1.1.3

**Location** PIM-GROUP-RP-MAPPING

## `rpop-bip-error-count`

**Description** Read-only. Indicates the number of Receive Path Overhead Processor (RPOP) Bit Interleaved Parity 8 (BIP-8) errors. The RPOP interprets pointers and extracts path overhead and the synchronous payload envelope. It is also responsible for path-level alarms and for monitoring performance.

**Usage** The `rpop-bip-error-count` value is read-only.

**Example** `rpop-bip-error-count = 0`

**Location** OC3-ATM-STAT

**See Also** `rlop-bip-error-count`, `rsop-bip-error-count`

## `rpop-febe-error-count`

**Description** Read-only. Indicates the number of Receive Path Overhead Processor (RPOP) Far End Block Errors (FEBEs).

**Usage** The `rpop-febe-error-count` value is read-only.

**Example** `rpop-febe-error-count = 0`

**Location** OC3-ATM-STAT

**See Also** `rlop-febe-error-count`

## `rsop-bip-error-count`

**Description** Read-only. Indicates the number of Receive Section Overhead Processor (RSOP) Bit Interleaved Parity 8 (BIP-8) errors. The RSOP synchronizes and descrambles frames, and provides section-level alarms and performance monitoring.

**Usage** The `rsop-bip-error-count` value is read-only.

**Example** `rsop-bip-error-count = 0`

**Location** OC3-ATM-STAT

**See Also** `rlop-bip-error-count`, `rpop-bip-error-count`

## `running-secs`

**Description** Read-only. Indicates the number of seconds that this inverse multiplexing over ATM (IMA) group has been in the operational state.

**Usage** The valid range for this read-only parameter is from 0 through 2147483647.

**Example** `running-secs = 53461`

**Location** IMA-GROUP-STAT

## rx-avail-cellrate

**Description** Read-only. Indicates the current cell rate (truncated value in cells per second) provided by this inverse multiplexing over ATM (IMA) group in the receive direction, considering all the receive links in the Active state.

**Usage** The valid range for this read-only parameter is from 0 through 2147483647.

**Example** rx-avail-cellrate = 0

**Location** IMA-GROUP-STAT

## rx-frame-length

**Description** Read-only. Indicates the value of inverse multiplexing over ATM (IMA) frame length as received from remote IMA function.

**Usage** Valid values for this read-only parameter are as follows:

| Option | Description                  |
|--------|------------------------------|
| 32     | IMA frame is 32 cells long.  |
| 64     | IMA frame is 64 cells long.  |
| 128    | IMA frame is 128 cells long. |
| 256    | IMA frame is 256 cells long. |

**Example** rx-frame-length = 128

**Location** IMA-GROUP-STAT

## rx-ima-id

**Description** Read-only. Indicates the inverse multiplexing over ATM (IMA) ID currently in use by the near-end IMA function.

**Usage** The valid range for this read-only parameter is from 0 through 255.

**Example** rx-ima-id = 0

**Location** IMA-GROUP-STAT

## rx-k1-byte-value

**Description** Read-only. Indicates the current value of the K1 byte received on the protection channel in the automatic protection switching (APS) system.

**Usage** The valid range for this read-only parameter is from 0 through 255.

**Location** APS-STAT

## rx-k2-byte-value

**Description** Read-only. Indicates the current value of the K2 byte received on the protection channel in the automatic protection switching (APS) system.

**Usage** The valid range for this read-only parameter is from 0 through 255.

**Location** APS-STAT

## rx-lid

**Description** Read-only. Indicates the receiving link identifier (Rx-Lid) of the link.

**Usage** The valid range for this read-only parameter is from 0 through 31.

**Example** rx-lid = 0

**Location** DS1-ATM-STAT:ima-link-status

## rx-lid-learning-time

**Description** *Not currently used.* Specifies the maximum amount of time in milliseconds allowed for learning the receiving link ID (the Rx Lid value) in IMA Control Protocol (ICP) cells.

**Usage** The valid range is from 0 through 2147483647. The default value is 100.

**Example** set rx-lid-learning-time = 100

**Location** DS1-ATM:line-config:ima-option-config:rxlink-config

## rx-min-num-links

**Description** Specifies the minimum number of receiving links to be active in order for the inverse multiplexing over ATM (IMA) group to remain in the operational state.

**Usage** Specify a number from 1 and 8. The default value is 1.

**Example** set rx-min-num-links = 1

**Location** IMAGROUP

## rxmt-interval

**Description** Pertains to Private Network-to-Network Interface (PNNI). Specifies the number of seconds between retransmissions of unacknowledged Database summary packets, PPNI Topology State Element (PTSE) Request packets, and PPNI Topology State Packets (PTSPs).

**Usage** Specify the number of seconds. The default value is 5.

**Example** set rxmt-interval = 5

**Location** PNMI-NODE-CONFIG[n]:node-timer

**See Also** peer-delayed-ack-interval  
ptse-holddown  
ptse-lifetime-factor  
ptse-refresh-interval

## rx-num-active-links

**Description** Read-only. Indicates the number of links that are configured to receive and are currently active in this inverse multiplexing over ATM (IMA) group.

**Usage** The valid range for this read-only parameter is from 0 through 24.

**Example** rx-num-active-links = 4

**Location** IMA-GROUP-STAT

## rx-num-config-links

**Description** Read-only. Indicates the number of links that are configured to receive in this inverse multiplexing over ATM (IMA) group.

**Usage** The valid range for this read-only parameter is from 0 through 24.

**Example** rx-num-config-links = 2

**Dependencies** The value of this parameter is overwritten by the value of the Tx-Num-Active-Links parameter in the ima-group-stat profile when the IMA group is configured in the SymmetricalConfiguration group symmetry mode.

**Location** IMA-GROUP-STAT

## rx-oam-label-value

**Description** Read-only. Indicates the inverse multiplexing over ATM (IMA) OAM Label value transmitted by the far end (FE) IMA unit. A value of 0 likely means that the IMA unit has not received an Administration, Operations, and Maintenance (OAM) label from the FE IMA unit at this time.

**Usage** The valid range for this read-only parameter is from 0 through 255.

**Example** rx-oam-label-value = 3

**Location** IMA-GROUP-STAT

## rx-sdu-size

**Description** Specifies the maximum ATM adaptation layer 5 (AAL5), common part convergence layer (CPCS), service data unit (SDU) size that is supported in the receive direction of this virtual channel connection (VCC).

**Usage** Specify the number of octets in a range for 0 to 65535. The default value is 0.

**Example** set rx-sdu-size = 32

**Location** ATM-VCL-CONFIG

## rx-signal-present

**Description** Read-only. Indicates whether the line is receiving signal from the remote end or not.

**Usage** Valid values for this read-only parameter are as follows:

- yes—Indicates that the local node is receiving a signal from the remote customer premises equipment (CPE).
- no—Indicates that the local node is not receiving a signal from the remote.

**Example** rx-signal-present = yes

**Location** AL-DMT-STAT:physical-statistic  
HDSL2-STAT:physical-statistic  
SDSL-STAT:physical-statistic  
SHDSL-STAT:physical-statistic

## rx-stuffs-counter

**Description** Read-only. Indicates the count of stuff events detected in the receive direction.

**Usage** The valid range for this read-only parameter is from 0 through 2147483647.

**Example** rx-stuffs-counter = 0

**Location** DS1-ATM-STAT:ima-link-statistic

**See Also** Elapsed-Seconds, Tx-Stuffs-Counter

## rx-test-pattern

**Description** Read-only. Indicates the test pattern received in the IMA control protocol (ICP) cell (octet 17) on the link during the inverse multiplexing over ATM (IMA) test pattern procedure.

**Usage** The valid range for this read-only parameter is from 0 through 255.

**Example** rx-test-pattern = 0

**Location** DS1-ATM-STAT:ima-link-status



## rx-testproc-status

**Description** Read-only. Indicates the current state of the test pattern procedure.

**Usage** Valid values for this read-only parameter are as follows:

- disabled—Test pattern procedure is currently disabled on this link.
- operating—Test pattern procedure is currently operating on this link.
- link-fail—Test pattern procedure has failed on this link.

**Example** rx-testproc-status = disabled

**Location** DS1-ATM-STAT:ima-link-status

## rx-timing-ref-link

**Description** Read-only. Indicates the index of the receive timing reference link.

This index is used by the near end for inverse multiplexing over ATM (IMA) data cell clock recovery. The Rx-Timing-Ref-Link is used to recover the clock from the physical layer and uses that recovered clock as a reference when it delivers cells to the higher layer, which is the ATM layer.

**Usage** Specify a number from 0 through 24. The distinguished value of zero may be used if no link has been configured in the IMA group, or if the receive timing reference link has not yet been detected.

**Example** rx-timing-ref-link = 1

**Location** IMA-GROUP-STAT

## rx-traffic-desc

**Description** The ATM traffic descriptor index applied to the receive direction of the virtual channel link (VCL).

**Usage** Specify a numeric value in the range 0 to 4294967295. The default value is 1.

**Example** set rx-traffic-desc = 100

**Location** ATM-VCL-CONFIG  
ATM-VPL-CONFIG

## S

### saal-retry-ms

**Description** In Asynchronous Transfer Mode (ATM), specifies the number of milliseconds allowed to lapse before retrying ATM adaptation layer (AAL) establish messages.

**Usage** Valid values are from 1000 to 5000.

**Example** `set saal-retry-ms = 10000`

**Location** ATM-IF-SIG-PARAMS [n] :q2931-options]

### save-level

**Description** Specifies the lowest level of log messages 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 Alert, and Emergency level are logged.

**Usage** Valid values are as follows:

| Value                           | Lowest-level message indicates                                                                                                                                                                                      |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>none</code>               | The Stinger unit does not display log messages.                                                                                                                                                                     |
| <code>emergency</code>          | The unit has an error condition and is unlikely to be operating normally.                                                                                                                                           |
| <code>alert</code>              | The unit has an error condition but is still operating normally.                                                                                                                                                    |
| <code>critical</code>           | An interface has gone down or a security error has occurred.                                                                                                                                                        |
| <code>error</code>              | An error event has occurred.                                                                                                                                                                                        |
| <code>warning</code>            | An unusual event has occurred, but the unit is otherwise operating normally. For example, this type of message appears when a login attempt has failed because the user entered an incorrect user name or password. |
| <code>notice</code>             | Events of interest in normal operation have occurred (a link going up or down, for example).                                                                                                                        |
| <code>info (the default)</code> | State and status changes that are commonly not of general interest have occurred.                                                                                                                                   |
| <code>debug</code>              | Helpful debugging information.                                                                                                                                                                                      |

**Example** `set save-level = error`

**Dependencies** Log levels are also configurable on a per-user basis in user profiles.

**Location** LOG

## save-number

**Description** Specifies the maximum number of log messages that the Stinger unit saves for display in the status windows.

**Usage** Specify an integer. The default is 100.

**Example** `set save-number = 150`

**Location** LOG

## scheduler-queue-size

**Description** On systems with an IP2000 control module the `scheduler-queue-size` parameter controls the per-queue threshold for traffic from the controller to a LIM.

**Usage** Valid values are from 100 through 10000. The default value is 200.

**Example** `set scheduler-queue-size = 400`

**Dependencies** The default setting of this parameter has been fine tuned to work for normal traffic conditions. Changing this value might result in random data traffic being discarded in extreme data traffic conditions.

Changes to the `scheduler-queue-size` parameter apply only to new connections that come up after this change. You must reset active connections for the new settings to apply.

**Location** SYSEEM

## scrambling-enabled

**Description** *Not currently used.* Specifies whether the payload of transmitted cells is scrambled or not.

**Usage** Valid values are as follows:

- `yes`—Enables the descrambling of received cells on the link. The payload of transmitted cells is scrambled.
- `no`—Disables the descrambling of received cells on the link. The payload of transmitted cells is not scrambled. This is the default.

**Example** `set scrambling-enabled = yes`

**Location** DS1-ATM:line-config

**See Also** `frame-type`

## screen-length

**Description** Specifies the number of lines displayed in the command-line window. (For the values to take effect, the user must log in again.)

**Usage** Specify a number from 24 to 999. The default is 24 lines.

**Example** `set screen-length = 68`

**Location** `USER`

**See Also** `status-length`

## screen-width

**Description** Specifies the screen width for all command line interface sessions subsequent to the current session.

**Usage** Specify a number from 80 (the default) to 255.

**Example** `set screen-width = 255`

**Location** `USER`

**See Also** `screen`

## sdsl-atm

**Description** Specifies whether code images for SDSL-48-Port Line Interface Modules (LIMs) should be stored in Flash memory.

**Usage** Valid values are as follows:

- `auto`—Causes the system to load images for cards that are installed in the Stinger unit, and to skip images for cards that are not installed. This is the default.
- `load`—Causes the system to load the image, even if there is no card of that type installed.
- `skip`—Causes the system to skip the image, even if there is a card of that type installed.

**Example** `set dsdl-atm = auto`

**Location** `LOAD-SELECT`

## sdsl-atm-v2

**Description** Specifies whether code images for SDSL-ATM-v2 cards should be stored in Flash memory.

**Usage** Valid values are as follows:

- `auto`—Causes the system to load images for cards that are installed in the Stinger unit, and to skip images for cards that are not installed. This is the default.
- `load`—Causes the system to load the image, even if there is no card of that type installed.
- `skip`—Causes the system to skip the image, even if there is a card of that type installed.

**Example** `set dsdl-atm-v2 = auto`

**Location** `LOAD-SELECT`

## sdtm

**Description** *Not used.*

**Location** BASE

## sealing-current-on

**Description** Enables or disables the sealing current function for testing purposes for all xDSL ports of the slot.

**Usage** Valid values are as follows:

- yes—Sets sealing current on.
- no (the default)—Sets sealing current off.

**Example** `set sealing-current-on = no`

**Dependencies** Currently only the SDSL and HDSL2 LIMs have the hardware to support sealing current for testing purposes.

The `xdsl-slot-config` profile is used to configure parameters at slot level that are common to all xDSL LIMs. By default, an `xdsl-slot-config` profile is created with an index of `[any-shelf any-slot 0]`. You can then create a profile for a particular slot with shelf 1 slot 0 as the index. The item number of the index must be 0.

**Location** XDSL-SLOT-CONFIG

**See Also** SLOT-INFO (profile)

## sec-domain-name

**Description** Specifies a secondary domain name to use for Domain Name System (DNS) lookups if the hostname is not found in the primary domain.

When specified in a `vrouter` profile, this DNS setting is exclusive to the virtual router. If DNS settings are not specified in a `vrouter` profile, the virtual router uses the DNS settings defined in the `ip-global` profile

**Usage** Specify a domain name.

**Example** `set sec-domain-name = eng.abc.com`

**Location** IP-GLOBAL

VROUTER

## secondary-controller-state-change-enabled

**Description** Enable or disables a trap (notification) when the secondary controller changes state.

**Usage** Valid values are as follows:

- **no**—Disables a trap when the secondary controller changes state. This is the default value.
- **yes**—Enables a trap when the secondary controller changes state.

**Example** `set secondary-controller-state-change-enabled = yes`

**Location** TRAP

## secondary-tunnel-server

**Description** Specifies the IP address or hostname of a secondary tunnel end point. If the primary server is unavailable, the system attempts to establish a tunnel to the secondary server.

**Usage** Specify the following, according to the tunneling protocol:

- For Layer 2 Tunneling Protocol (L2TP) tunneling, optionally specify the address or name of a secondary L2TP network server (LNS).
- For Ascend Tunnel Management Protocol (ATMP) tunneling, optionally specify the address or name of a secondary Home Agent.

**Example** `admin> set secondary-tunnel-server = 3.3.3.3/24`

In an ATMP mobile-client profile, the value can include a UDP port number, which must match the UDP port specified in the Home Agent atmp profile. For example,

`admin> set secondary-tunnel-server = 3.3.3.3:1155`

**Dependencies** If you specify a hostname and a DNS lookup returns several IP addresses, the system attempts to establish a tunnel to each address in turn.

**Location** CONNECTION:tunnel-options

## seconds-history

**Description** Specifies the number of seconds to use as the basis for calculating average line utilization (ALU).

When the ALU exceeds or falls below the target-utilization percentage for a specified number of seconds, the Stinger unit adds or subtracts bandwidth.

**Usage** Specify an integer from 1 to 300. The default is 15 seconds.

The number of seconds you specify must be related to traffic patterns. For example, if you want to average spikes with normal traffic flow, you might want the Stinger unit to base ALU on a longer time period. If, on the other hand, traffic patterns consist of many spikes that are short in duration, you might want to specify a shorter period of time to give less weight to the short spikes.

**Example** set seconds-history = 60

**Location** ANSWER-DEFAULTS:mpp-answer  
CONNECTION STATION:mpp-options

**See Also** target-utilization

## section-state

**Description** Read-only. Indicates the state of the SONET section. A SONET section is a single run of cable. Section-terminating equipment is any adjacent pair of switches.

**Usage** The section-state value is read-only. Valid values are as follows:

- sonet-disabled—SONET is disabled.
- sonet-section-active-no-defect—SONET section is active with no defect.
- sonet-section-loss-of-signal—SONET section is in a loss-of-signal state.
- sonet-section-loss-of-frame—SONET section is in a loss-of-frame state.

**Example** section-state = sonet-section-active-no-defect

**Location** OC3-ATM-STAT

## security-enabled

**Description** Specifies whether the Stinger unit traps security events and sends a trap (notification) protocol data unit (PDU) to the Simple Network Management Protocol (SNMP) manager. Security events notify users of security problems and track access to the unit.

The Stinger unit can trap the following security events:

| Event          | Indication                                                                                                                                        |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| authentication | An authentication failure occurred.                                                                                                               |
| console        | Console associated with the passed console index has changed state. To read the console's state, get ConsoleEntry from the Ascend Enterprise MIB. |
| useexceeded    | Specific port has exceeded the number of DS0 minutes allocated to it.                                                                             |

**Usage** Valid values are as follows:

- yes—Specifies that the Stinger unit sends security-event traps to the host specified by host-address.
- no—Specifies that the Stinger unit does not send security-event traps. This is the default.

**Example** set security-enabled = yes

**Location** TRAP

## security-level

**Description** Specifies the level of security to use when generating messages.

**Usage** Valid values are as follows:

- `none`—Specifies no authentication and no privacy. This is the default.
- `auth-nopriv`—Specifies authentication and no privacy.
- `auth-priv`—Specifies authentication and privacy.

**Example** `set security-level = auth-priv`

**Dependencies** Consider the following:

- For `auth-priv` to apply, you must set the `priv-protocol` and `priv-password` parameters in the `snmpv3-usm-user` profile.
- When you specify the `auth-priv` setting, all user transmissions with a security level of `none` or `auth-nopriv` are rejected with the error message `Unsupported Security Level`.

**Location** `SNMP`  
`SNMPV3-TARGET-PARAM`

## security-mode

**Description** *Not used.*

## security-model

**Description** Specifies the security model to use when generating SNMP messages.

**Usage** Valid values are as follows:

- `v1`—Specifies the SNMP version 1 security model. This is the default.
- `v3-usm`—Specifies the SNMP version 3 User-Based Security Model (USM). For SNMPv3 Notifications support, specify `v3-usm`. Specify this value for view-based access control model (VACM) support

**Example** `set security-model = v3-usm`

**Dependencies** Consider the following:

- You can specify `v1` only when you have also set `Msg-Proc-Model` to `V1`.
- You can specify `v3-usm` only when you set `Msg-Proc-Model` to `V3`.
- When `security-model` is set to `v3-usm`, you must configure an `snmpv3-usm-user` profile, with the name specified for the `security-name` parameter, in order for the `snmpv3-target-param` profile to have any effect.

**Location** `SNMPV3-TARGET-PARAM`  
`VACM-SECURITY:security-properties`



## security-name

**Description** Specifies a name used in Simple Network Management Protocol (SNMP) version 3 USM. The security name identifies the user on whose behalf SNMPv3 USM messages are generated.

**Usage** Specify up to 22 characters. The default is null.

**Example** `set security-name = newuser`

**Dependencies** Security-Name applies only if Security-Model is set to V3-USM.

**Location** `SNMPV3-TARGET-PARAM`  
`VACM-SECURITY:security-properties`

## selection-end

**Description** Read-only. Indicates the time at which the controller in this context detected the end of remote selection.

**Usage** Read-only parameter with a numeric range of 0 to 4294967295.

**Example** `selection-end = 123`

**Location** `REDUNDANCY-STATS:context-stats`

## selection-start

**Description** Read-only. Indicates the time at which the controller in this context selected a function.

**Usage** Read-only parameter with a numeric range of 0 to 4294967295.

**Example** `selection-start = 123`

**Location** `REDUNDANCY-STATS:context-stats`

## select-reason

**Description** Read-only. Indicates the basis on which the controller in this context was assigned the current function.

**Usage** Read-only parameter with the following possible values:

- `defer-to-running-primary`
- `no-running-primary`
- `single-controller-operation`
- `local-primary-preference`
- `remote-primary-preference`
- `local-crash`
- `remote-crash`
- `local-local-local-error`

- remote-local-local-error
- local-remote-local-error
- remote-remote-local-error
- local-matches-chassis
- remote-matches-chassis
- prior-pair-function
- local-primary-resources
- remote-primary-resources
- local-secondary-resources
- remote-secondary-resources
- prior-local-primary
- prior-remote-primary
- local-crash-history
- remote-crash-history
- local-local-local-error-history
- remote-local-local-error-history
- local-remote-local-error-history
- remote-remote-local-error-history
- local-slot-number
- remote-slot-number
- contention-resolution
- unable-to-acquire-buses
- communication-loss

**Location** REDUNDANCY-STATS:context-stats

## self-test

**Description** Read-only. Indicates whether the module has passed the power-on self test (POST).

**Usage** Valid values for this read-only parameter are as follows:

- passed—Indicates that the module passed the POST.
- failed—Indicates that the module failed the POST.

**Example** self-test = passed

**Location** AL-DMT-STAT:physical-statistic  
HDSL2-STAT:physical-statistic  
SDSL-STAT:physical-statistic  
SHDSL-STAT:physical-statistic

## send-auth-mode

**Description** Specifies the authentication protocol the system uses to send a password to the calling device during bidirectional Challenge Handshake Authentication Protocol (CHAP) authentication.

**Usage** Specify one of the following values:

- `no-ppp-auth` (the default)—Does not use bidirectional authentication.
- `pap-ppp-auth`—Not supported for bidirectional CHAP.
- `chap-ppp-auth`—Uses CHAP to send a password to the calling device.
- `ms-chap-ppp-auth`—Uses Microsoft's extension of CHAP, designed mostly for Windows NT and LAN Manager platforms.

**Example** `set send-auth-mode = chap-ppp-auth`

**Dependencies** Bidirectional authentication is applicable only if the send authentication mode is CHAP or MS-CHAP. These settings are used only when `bi-directional-auth` is enabled.

**Location** `CONNECTION:ppp-options`

## send-code

**Description** Specifies the type of code pattern to send to the DS1-ATM interface.

**Usage** Following are the valid values:

- `no-code` (the default)—Sends looped or normal data.
- `line-code`—Sends a request for a line loopback.
- `payload-code`—Sends a request for a payload loopback.
- `reset-code`—Sends a loopback termination request.
- `qrs-code`—Sends a quasi-random signal (QRS) test pattern.
- `511-pattern`—Sends a 511-bit fixed-test pattern.
- `3-in-24-pattern`—Sends a fixed test pattern of 3 bits set in 24.
- `1-in-16-pattern`—Sends a fixed test pattern of 1 bit set in 16.
- `all-ones-pattern`—Sends a fixed test pattern of all ones.
- `all-zeros-pattern`—Sends a fixed test pattern of all zeros.
- `alt-ones-zeros-pattern`—Sends a fixed test pattern of alternating ones and zeros.
- `dbl-alt-ones-zeros-pattern`—Sends a fixed test pattern of double alternating ones and zeros.
- `2-pow-20-pattern`—Sends the pseudorandom pattern type ( $2^{20} - 1$ ) (ITU-T recommendation O.151).

**Example** `set send-code = 1-in-16-pattern`

**Location** `DS1-ATM:line-config`

**See Also** `frame-type`, `line-interface`, `fdl`

## send-code-status

**Description** Specifies the current state of the Send-Code sent over a DS1 line.

**Usage** The following are valid values:

- `disabled`—Specifies that the SendCode procedure is currently disabled on this link.
- `line-loopback`—Specifies that line loopback has been requested to the remote end
- `payload-loopback`—Specifies that payload loopback has been requested to the remote end

**Example** `set send-code-status = line-loopback`

**Location** `DS1-ATM-STAT {shelfN slotN N}`

**See Also** `fdl`, `pattern-test-status`

## send-icmp-dest-unreachable

**Description** *Not supported.* Specifies whether the unit sends Internet Control Message Protocol (ICMP) destination-unreachable packets. Setting this parameter to `no` can break required behavior for IPv4 routers, such as path MTU discovery. It is intended for use only in voice over IP applications.

**Location** `IP-GLOBAL`

## send-password

**Description** Specifies the password the system sends to the calling device during bidirectional Challenge Handshake Authentication Protocol (CHAP) authentication.

**Usage** Specify up to 20 characters. The password is case sensitive.

**Example** `set send-password = unit0`

**Dependencies** Bidirectional authentication is applicable only if the send authentication mode is CHAP or MS-CHAP. These settings are used only when `bi-directional-auth` is enabled.

**Location** `CONNECTION:ppp-options`

## serial-number

**Description** Read-only. Displays the unit's serial number.

**Usage** The serial-number setting is read-only.

**Example** serial-number = 6201732

**Location** BASE  
SLOT-INFO

**See Also** software-level, software-revision, software-version

## server-auth-id

**Description** Specifies the Layer 2 Tunneling Protocol (L2TP) network server (LNS) system name used for tunnel authentication. This name is sent to the L2TP access concentrator (LAC) in Start-Control-Connection-Reply (SCCRP) packets.

**Usage** Specify up to 31 characters. The default is null.

**Example** set server-auth-id = caserver

**Dependencies** This setting is currently ignored if specified in a connection profile.

**Location** CONNECTION:tunnel-options  
TUNNEL-SERVER

## server-endpoint

**Description** Specifies the IP address or hostname of the Layer 2 Tunneling Protocol (L2TP) network server (LNS). Usually, this is the same value as the Tunnel-Server-Endpoint RADIUS attribute, but it can differ.

**Usage** Specify a hostname or IP address. The default is the null address. If you specify a hostname, the system performs a Domain Name System (DNS) lookup for the IP address. The default is null.

**Example** set server-endpoint = 1.1.1.1

**Location** TUNNEL-SERVER

## service

**Description** Not used.

**Location** TERMINAL-SERVER

## service-name

**Description** Name assigned to multicast service.

**Usage** Specify up to 31 alphanumeric characters. The default is null.

**Example** `set service-name = gold`

**Location** `MCAST-SERVICE`

## service-type

**Description** Type of service for the traffic flow of the connection.

**Usage** Valid values are as follows:

- `none` (the default)—The profile has no effect on traffic flows if applied to a connection profile.
- `vlan-stack-user-tag`—Enable the system to map the VLAN tag in the incoming traffic flow to a different VLAN user ID for stacked VLANs.

**Example** `set service-type = vlan-stack-user-tag`

**Location** `FLOW-SERVICES`

## ses-adsl-dmt-down-rate

**Description** Specifies the per-session ADSL DMT downstream data rate, in bits per second.

**Usage** Valid values are as follows:

128000  
256000  
384000  
512000  
640000  
768000  
960000  
1280000  
1600000  
1920000  
2240000  
2560000  
2688000  
3200000  
4480000  
5120000  
6272000  
7168000  
8000000—This is the default.  
8960000  
9504000  
auto

**Example** `set ses-adsl-dmt-down-rate = 9504000`

**Location** `CONNECTION:session-options`

## ses-adsl-dmt-up-rate

**Description** Specifies the per-session ADSL DMT downstream data rate, in bits per second.

**Usage** Valid values are as follows:

128000  
256000  
384000  
512000  
640000  
768000  
800000  
896000  
928000—This is the default.  
1088000  
auto

**Example** set ses-adsl-dmt-up-rate = 800000

**Location** CONNECTION:session-options

## ses-rate-mode

**Description** Specifies the DSL data rate mode for the connection.

**Usage** Select one of the following values:

- autobaud (the default)—Specifies that a DSL modem should train up to a set data rate. If a DSL modem cannot train to this data rate, it connects to the closest rate to which it can train (the modem's ceiling rate).
- singlebaud—Causes the system to train to a single data rate, even if the DSL modem can train at a higher or lower data rate. If the DSL modem cannot train to the specified single rate, the connection fails.

**Example** set ses-rate-mode = singlebaud

**Location** CONNECTION:session-options

## ses-rate-type

**Description** Specifies the per-session modem type for rate control.

**Usage** Valid values are as follows:

- disabled (the default)—Specifies that modem rate control is not active for the connection.
- SDSL—Specifies SDSL modem rate control.
- adsl-dmt-cell—Specifies ADSL modem rate control.

**Example** set ses-rate-type = sdsl

**Location** CONNECTION:session-options

## ses-sdsl-rate

**Description** Specifies the symmetrical data rate. This setting applies to connections on the SDSL LIM.

**Usage** Specify one of the following values:

144000  
160000  
192000  
208000  
272000  
384000  
400000  
416000  
528000  
768000  
784000  
1040000  
1152000  
1168000  
1536000  
1552000  
1568000  
1680000  
1920000  
2160000  
2320000

**Example** `set ses-sdsl-rate = 1552000`

**Location** `CONNECTION:session-options`

**See Also** `Ses-Rate-Type`

## session-id

**Description** ID number of the user session.

**Usage** This parameter is read-only.

**Example** `session-id = 2`

**Location** `cmd-log`



## sessionid-base

**Description** Specifies the base number the Stinger unit uses for generating a unique ID for each session.

The Stinger unit can pass a session ID to SNMP, RADIUS, or other external entities. If the value of SessionID-Base is nonzero, the Stinger unit uses it as the initial base for calculating session IDs after a system reset. The ID for each subsequent session is incremented by 1. If SessionID-Base is zero, the Stinger unit sets the initial base for session IDs to the absolute clock. For example, if the clock is 0x11cf4959, the subsequent session IDs use 0x11cf4959 as a base. However, if the clock is changed and the system reboots or clears NVRAM, session IDs might be duplicated.

**Usage** Specify an integer from 1 to 2147483647. The default is 0 (zero), which causes the Stinger unit to use the absolute clock to generate a session ID base.

**Example** `set sessionid-base = 0`

**Dependencies** You can also set a session ID base by using the Set SessID command in the terminal-server interface. The terminal server provides a Show SessID command to display the next session ID the unit will use.

**Location** SYSTEM

## severely-errored-second

**Description** Read-only. Indicates the number of 1-second intervals during which at least 50 cyclic redundancy check (CRC) anomalies are declared or one or more loss of synchronous word (LOSW) defects are declared.

**Usage** The severely-errored-second setting is a read-only display for checking operations.

**Example** `severely-errored-second = 1`

**Location** HDLSL2-STAT:physical-statistic  
SHDSL-STAT:physical-statistic

**See Also** errored-second, losw-second, unavailable-second

## shared-prof

**Description** Enables or disables multiple callers sharing a single connection profile. Sharing profiles is recommended only for *low-security* networks.

Sharing profiles can be enabled on two levels: globally in the ip-global profile, or connection-specific in a connection profile. Once you enable shared profiles globally, you cannot disable it for an individual connection. However, if you disable shared profiles globally, you can enable it for specific connections only. This functionality is also available in RADIUS profiles via the ascend-shared-profile-enable attribute.

**Usage** Valid values are as follows:

- **yes**—Allows more than one caller to share the same profile and password, provided that no IP address conflicts result.
- **no** (the default)—Does not allow shared profiles.

**Example** `set shared-prof = no`

**Dependencies** Profiles with a hard-coded remote IP address cannot be shared.

**Location** CONNECTION  
IP-GLOBAL

## shared-secret

**Description** Specifies a value used by both the Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) and the L2TP network server (LNS) ends of an L2TP tunnel to authenticate tunnel requests initiated by local `connection` profiles.

**Usage** Specify the text of the shared secret, up to 21 characters. The default is null.

**Example** `set shared-secret = 3f4tr`

**Location** TUNNEL-SERVER

## share-global-pool

**Description** Enables or disables the ability of a virtual router to share the address pools configured in the `ip-global` profile.

When this feature is enabled, a virtual router can use its own address pools, which are configured in its `vrouter` profile, but cannot assign addresses from the pools defined in the `ip-global` profile.

**Usage** Valid values are as follows:

- **yes** (the default)—If no address pools are configured for the virtual router, or if its pools have no free addresses, a `connection` profile in the virtual router's domain can be assigned an IP address from the pool defined in the `ip-global` profile.
- **no**—If no address pools are configured for the virtual router, or if its pools have no free addresses, `connection` profile in the virtual router's domain that requires dynamic address assignment are unable to establish a connection.

**Example** `set share-global-pool = no`

**Location** VROUTER

## shelf

**Description** Specifies or indicates, according to the profile, the shelf in which an item resides. The shelf number is always 1 for Stinger units.

**Usage** For a device-address or physical-address profile, specify the integer 1. In an error profile, the shelf setting is read-only.

**Example** `set shelf = 1`

**Location** cmd-log  
DEVICE-ADDRESS  
ERROR  
PHYSICAL-ADDRESS

## shelf-controller-type

**Description** The shelf-controller-type configures the unit to initialize operation in the appropriate mode.



**Note** After a unit's shelf-controller-type has been changed, it must be reset for the change to become effective.

**Usage** Valid values are as follows:

- standalone (the default)—Configures the shelf to operate in standalone mode. This is a valid value for a Stinger control module (CM) or Stinger micro-remote terminal (MRT).
- master—Configures the host shelf to serve as the master controller. This is a valid value for a Stinger CM or Stinger MRT.
- slave—Configures a remote shelf to operate in slave mode. This is a valid value for a Stinger compact remote terminal (CRT) or Stinger MRT.

**Example** `set shelf-controller-type = master`

**Dependencies** A user can not change the value of shelf-controller-type to standalone if at least one remote-shelf-config profile was configured. All remote-shelf-config profiles must be deleted before this change is allowed.

**Location** SYSTEM

## shelf-number

**Description** Read-only. Indicates the shelf number of the Stinger unit.

**Usage** The shelf-number is always 1 for Stinger units.

**Example** `shelf-number = 1`

**Location** BASE  
FRDLCI-STAT

## short-location

**Description** Specifies the distance detected to the short circuit in a copper loop test (CLT).

**Usage** Specify the number of units. The distance is reported in centimeters if units are set to metric. The distance is reported in hundredths of feet if units are set to English. The default value of 0 (zero) specifies that no short circuit is to be detected.

**Example** `set short-location = 52`

**Dependencies** The `shortloc-unit` parameter must be set to the appropriate unit to make `short-location` effective.

**Location** CLT-RESULT

## shortloc-gauge

**Description** Specifies the gauge of the cable in the loop of a copper loop test (CLT).

**Usage** Valid values are as follows:

- In English units, the value is 22, 24, or 26 AWG.
- In metric units, the value is 4, 5, or 6 tenths of a millimeter.

**Example** `set shortloc-gauge = 4`

**Dependencies** The `shortloc-unit` parameter must be specified correctly to make the `shortloc-gauge` parameter effective.

**Location** CLT-COMMAND

## shortloc-type

**Description** Specifies the type of short circuit test in a copper loop test (CLT).

**Usage** Valid values are as follows:

- `detect`—Short circuit detection occurs prior to the measurement of the short circuit location. This is the default value.
- `nodet`—Short circuit detection does not occur prior to the measurement of the short circuit location.

**Example** `set shortloc-type = detect`

**Location** CLT-COMMAND

## shortloc-unit

**Description** Specifies the units of measurement for short circuit location test in a copper loop test (CLT).

**Usage** Valid values are as follows:

- `english`—English units are used for the measurement.
- `metric`—Metric units are used for the measurement. This is the default value.

**Example** `set shortloc-unit = metric`

**Dependencies** The `shortloc-gauge` parameter must be specified correctly to make the `shortloc-unit` parameter effective.

**Location** `CLT-COMMAND`

## signalling-state

**Description** Read-only. Indicates the signaling state of the port.

**Usage** Valid values are as follows:

- `not-configured`—The component is not configured.
- `up`—The component is in an up state.
- `down`—The component is in a down state.

**Example** `signalling-state = up`

**Location** `ATM-IF-STAT`

**See Also** `pnmi-link-state`, `port-state`

## sig-vcc-rx-qos-name

**Description** Name of the quality-of-service (QoS) contract (`atm-qos` profile) used during Integrated Local Management Interface (ILMI) autoconfiguration to specify the advertised signaling virtual channel connection (VCC) traffic parameters for the receive direction. *ILMI is not supported with the current software version.*

**Usage** Enter up to 31 alphanumeric characters. You can specify the name of any configured `atm-qos` profile. The default value is `default-ctl`.

**Example** `set sig-vcc-rx-qos-name = rx-ctl`

**Location** `ATM-IF-CONFIG:extension-config`

## sig-vcc-rx-tdesc-index

**Description** *ILMI is not currently used.* Specifies the traffic descriptor index which is used during the Integrated Local Management Interface (ILMI) autoconfiguration to specify the advertised signaling virtual channel connection (VCC) traffic parameters for the receive direction.

**Usage** The default value of 2 specifies the default-ctl traffic descriptor used for Private Network-to-Network Interface (PNNI) signaling and routing control.

**Example** `sig-vcc-tx-tdesc-index = 2`

**Location** ATM-IF-CONFIG:extension-config

## sig-vcc-tx-qos-name

**Description** Name of the quality-of-service (QoS) contract (atm-qos profile) used during ILMI autoconfiguration to specify the advertised signaling virtual channel connection (VCC) traffic parameters for the transmit direction. *ILMI is not supported with the current software version.*

**Usage** Enter up to 31 alphanumeric characters. You can specify the name of any configured atm-qos profile. The default value is default-ctl.

**Example** `set sig-vcc-tx-qos-name = tx-ctl`

**Location** ATM-IF-CONFIG:extension-config

## sig-vcc-tx-tdesc-index

**Description** *ILMI is not currently used.* Specifies the traffic descriptor index used during Integrated Local Management Interface (ILMI) autoconfiguration to specify the advertised signaling virtual channel connection (VCC) traffic parameters for the transmit direction.

**Usage** The default value of 2 specifies the default-ctl traffic descriptor used for Private Network-to-Network Interface (PNNI) signaling and routing control.

**Example** `set sig-vcc-rx-tdesc-index = 2`

**Location** ATM-IF-CONFIG:extension-config

## silent-mode

**Description** *Not used.*

**Location** TERMINAL-SERVER:terminal-mode-configuration

## single-file-incoming

**Description** Specifies whether the Stinger unit treats incoming calls as a single-file list, or handles them in parallel.

**Usage** Valid values are as follows:

- **yes**—Specifies that the Stinger unit answers and routes one call before answering and routing the next call. This is the default.
- **no**—Specifies that the Stinger unit answers and routes an incoming call immediately.

**Example** `set single-file-incoming = yes`

**Location** `SYSTEM`

**See Also** `parallel-dialing`

## site-minus-1

**Description** *Not currently used.* Specifies the number representing the highest level of the Private Network-to-Network Interface (PNNI) hierarchy that lies within the site, minus one scope.

**Usage** Specify a number from 0 to 104. The default value is 80.

**Example** `set site-minus-1 = 80`

**Location** `PNNI-NODE-CONFIG [n] :node-scope-mapping`

## site-plus-1

**Description** *Not currently used.* Specifies the number representing the highest level of the Private Network-to-Network Interface (PNNI) hierarchy that lies within the site, plus one scope.

**Usage** When this parameter becomes available, you will be able to specify a number from 0 to 104. The default value is 72.

**Example** `set site-plus-1 = 72`

**Location** `PNNI-NODE-CONFIG N:node-scope-mapping`

**See Also** `intra-site`  
`local-net`  
`local-net-plus-1`

## slip

**Description** *Not used.*

**Location** `TERMINAL-SERVER:slip-mode-configuration`

## slip-bootp

**Description** *Not used.*

**Location** `TERMINAL-SERVER:slip-mode-configuration`

## slot

**Description** Specifies or indicates, depending on the profile, the number of an item's expansion slot. Stinger slots are numbered as follows:

- In a Stinger FS or Stinger FS+, the line interface module (LIM) slots are numbered from 1 to 16, with slots 8 and 9 reserved for the control module(s). Slots 17 and 18 are reserved for the trunk modules.
- in a Stinger LS or Stinger RT, the LIM slots are numbered from 1 to 5 for the model 1 chassis, and from 1 to 7 for the model 2 chassis. Slots 8 and 9 are reserved for the control module(s). Slots 17 and 18 are reserved for the trunk modules.
- In a Stinger MRT, the built-in LIM operates from virtual slot 1. The built-in controller operates from virtual slot 8. The built-in trunk module operates from slot 17, and the plug-in trunk module operates from slot 18.

**Usage** For a `device-address` or `physical-address` setting, specify an integer from 1 to 18. In an error profile, the slot setting is read-only.

**Example** `set slot = 10`

**Location** `cmd-log`  
`DEVICE-ADDRESS`  
`ERROR`  
`PHYSICAL-ADDRESS`

## slot-address

**Description** Indicates or specifies the physical address of the slot.

**Usage** For any Stinger unit, the shelf number is always 1. Stinger slots are numbered as follows:

- In a Stinger FS or Stinger FS+, the line interface module (LIM) slots are numbered from 1 to 16, with slots 8 and 9 reserved for the control modules (CM). Slots 17 and 18 are reserved for the trunk modules.
- In a Stinger LS or Stinger RT, the LIM slots are numbered from 1 to 5 for the model 1 chassis and 1 to 7 for the model 2 chassis. Slots 8 and 9 are reserved for the control modules. Slots 17 and 18 are reserved for the trunk modules.
- In a Stinger MRT, the built-in LIM operates from virtual slot 1. The built-in control module operates from virtual slot 8. The built-in trunk module operates from slot 17, and the plug-in trunk module operates from slot 18.

In most cases, the value of `slot-address` is obtained from the system. However, you can clone a profile by reading an existing one and changing its physical address.



**Example** Use the following examples to help you:

- To modify the value after reading a slot-info, slot-state, or slot-type profile, use the list and set commands. For example:

```
admin> list slot-address
[in SLOT-INFO/{ shelf-1 slot-9 37 }:slot-address]
shelf=shelf-1
slot=slot-9
item-number=37

admin> set shelf = shelf-2
```

- As an alternative, you can simply use the set command:

```
admin> set slot-address shelf = shelf-2
```

**Location** SLOT-INFO

SLOT-STATE

SLOT-TYPE

**See Also** physical-address

## slot-cac-enable

**Description** Enable/disable connection admission control (CAC) on the line interface module (LIM) slot. Slot-level CAC is enabled by default with this new setting.

**Usage** Valid values are as follows:

- yes (the default)—CAC on the LIM slot is enabled.
- no—CAC on the LIM slot is disabled.

**Example** set slot-cac-enable = no

**Location** SLOT-STATIC-CONFIG

## slot-enabled

**Description** Specifies whether the Stinger unit traps changes of state in a host interface and sends a trap (notification) protocol data unit (PDU) to the Simple Network Management Protocol (SNMP) manager.

**Usage** Valid values are as follows:

- yes—Specifies that the Stinger unit sends a trap PDU to the host specified by host-address.
- no (the default)—Specifies that the host does not receive a trap.

**Example** set slot-enabled = yes

**Location** TRAP

## slot-number

**Description** Read-only. Indicates the slot number of the line interface module (LIM) or trunk module on a Stinger unit owning the virtual channel connection (VCC) on an Asynchronous Transfer Mode (ATM) link.

**Usage** The slot-number value is read-only, and can be one of the following:

Any-Slot

Slot-1

Slot-2

Slot-3

Slot-4

Slot-5

Slot-6

Slot-7

Control-Module-1—Primary control module (CM) slot

Control-Module-2—Secondary control module (CM) slot

Slot-10

Slot-11

Slot-12

Slot-13

Slot-14

Slot-15

Slot-16

Trunk-Module-1—Trunk module 1 pseudo-slot

Trunk-Module-2—Trunk module 2 pseudo-slot

Slot-Forward—Control module forward pseudo-slot

**Example** set slot-number = slot-10

**Location** ATMPVC-STAT:vcc-members:vcc members [n]

ATMVCC-STAT:vcc-ident

FRDLCI-STAT

## slot-over-subscription

**Description** Specifies oversubscription to a LIM slot's provisioned guaranteed upstream bandwidth.

**Usage** Integer value from 0 to 10,240. The default value is 10. A value of zero disables slot CAC.

**Example** set slot-cac-oversubscription = 5000

**Location** SLOT-STATIC-CONFIG

slot-profile-change-enabled

**Description** Specifies whether the system generates a trap (notification) when a slot-state profile changes.

A trap indicates that a slot-state profile has been created as a result of slot insertion, or that a slot state has transitioned to oper-state-down, oper-state-up, oper-state-dump, or oper-state-none.

**Usage** Valid values are as follows:

- yes—Specifies that the system generates a trap. This is the default.
- no—Specifies that the system does not generate a trap.

**Example** set slot-profile-change-enabled = no

**Location** TRAP

**See Also** current-state  
slot-type

slot-type

**Description** Read-only. Indicates the type of device in the slot. If the actual type of device identified by the system at startup differs from the type indicated by slot-type, the Stinger unit determines that you have changed slot cards. It then deletes the old Simple Network Management Protocol (SNMP) interface numbers.

**Usage** Valid values are as follows:

| Value                       | Indicates                                |
|-----------------------------|------------------------------------------|
| cm                          | Control module in slot 8 and 9.          |
| dadsl-atm-24-card           | 24-port DMT ADSL ATM LIM.                |
| ds3-atm2-card               | DS3-ATM trunk module.                    |
| ds3-atm-card                | DS3-ATM module.                          |
| ds3-atm-trunk-daughter-card | DS3-ATM trunk daughter module.           |
| e3-atm-card                 | E3-ATM trunk module                      |
| e3-atm-trunk-daughter-card  | E3-ATM trunk daughter module.            |
| glite-atm-48-card           | 48-port G-lite ADSL LIM.                 |
| hdsl2-card                  | 32-port SHDSL/HDSL2 LIM.                 |
| ima-24-e1-card              | 24-port E1 module.                       |
| ima-24t1-card               | 24-port T1 module.                       |
| ima-8-e1-card               | 8-port E1 module.                        |
| ima-8-t1-card               | 8-port T1 module                         |
| mrt-36-adsl-card            | Stinger MRT ADSL ports                   |
| none                        | No module present in the addressed slot. |

| Value                       | Indicates                      |
|-----------------------------|--------------------------------|
| oc3-atm-card                | OC3-ATM trunk module.          |
| oc3-atm-trunk-daughter-card | OC3-ATM trunk daughter module. |
| router-card                 | T1000 module.                  |
| sdsl-atm-v2-card            | 48-port SDSL v2 LIM.           |
| stngr-40a-adsl-card         | 40-port ADSL CT Annex A LIM.   |
| stngr-48a-adsl-card         | 48-port ADSL Annex A LIM.      |
| stngr-48b-adsl-card         | 48-port ADSL Annex B LIM.      |
| stngr-48c-adsl-card         | 48-port ADSL Annex C LIM.      |

**Example** slot-type = dadsl-atm-24-card

**Dependencies** You can also display the slot type for a particular device by using the terminal-server Show command.

**Location** ADMIN-STATE-PHYS-IF  
SLOT-TYPE

**See Also** slot  
slot-address  
SLOT-INFO  
slot-type

## slot-vpi-vci-range [n]

**Description** *Deprecated and not used.*

**Location** ATM-CONFIG:slot-vpi-vci-range

**See Also** SLOT-STATIC-CONFIG

## snext-margin

**Description** Specifies the amount of compensation for self-noise generated by adjacent SHDSL lines in the same bundle. A value other than disable reduces the maximum rate that the loop trains at.

**Usage** Valid values are as follows:

0db  
1db  
2db  
3db  
4db  
5db  
6db  
7db  
8db

9db  
10db  
-10db  
-9db  
-8db  
-7db  
-6db  
-5db  
-4db  
-3db  
-2db  
-1db  
disable (the default)

**Example** set snext-margin = 3db

**Dependencies** This parameter applies only if the rate-mode parameter is set to auto-mode.

**Location** HDLSL2:line-config  
SHDSL:line-config

## snmp-illegal-access-attempt

**Description** Enables or disables the Ascend security alert trap (notification).

**Usage** Select one of the following values.

- no—Disables the Ascend security alert trap. This is the default value.
- yes—Enables the Ascend security alert trap.

**Example** set snmp-illegal-access-attempt = yes

**Location** TRAP

## snmp-interface

**Description** Read-only. Indicates the Simple Network Management Protocol (SNMP) interface number assigned to the device by the system.

At system startup, the Stinger unit reads the admin-state-perm-if and admin-state-phys-if profiles. If the addressed device is not present in the system and has been replaced by a device of another type, the unit deletes the profile associated with the device. The next time the unit is reset or powered off and on, the old device's SNMP interface number is made available for reassignment.

Removing a module and leaving the slot empty, however, does not free up interface numbers. If you reinstall the module, the unit reassigns the same interface number. In addition, removing a module and replacing it with a module of another type does not immediately free up the old interface numbers. New numbers are assigned to the new module, and the old numbers become available at the next power cycle or system reset.

**Usage** The SNMP-Interface setting is read-only.

**Example** `snmp-interface = 65`

**Location** ADMIN-STATE-PERM-IF  
ADMIN-STATE-PHYS-IF

**See Also** SNMP (profile)

## snmp-message-type

**Description** Specifies the version of Simple Network Management Protocol (SNMP) used by the SNMP agent in the unit.

**Usage** Valid values are as follows:

- `v1-and-v3`—Causes the SNMP agent to use both SNMPv1 and SNMPv3 protocols. This is the default.
- `v1-only`—Causes the SNMP agent to use only the SNMPv1 protocol and discard any other types of messages.
- `v3-only`—Causes the SNMP agent to use only the SNMPv3 protocol and discard other types of messages.

**Example** `set snmp-message-type = v3-only`

**Location** SNMP-MANAGER

**See Also** Security-Level

## snmp-trap-enable

**Description** *Deprecated and not used.*

**Location** MCAST-SERVICE

## snr-margin

**Description** Read-only. Indicates the signal-to-noise ratio on the line, in decibels. The signal-to-noise ratio defines a relationship between the noise floor and the signal.

**Usage** The `snr-margin` setting is read-only.

**Example** `snr-margin = 40`

**Dependencies** Line quality of 24dB or higher is required for reliable data transfer..

**Location** SHDSL-STAT:physical-statistic

## soft-ip-interface-addr

**Description** *Deprecated and not used.*

**See Also** IP-INTERFACE

## software-debug

**Description** Enables or disables software debug message logging.

**Usage** Select one of the following values:

- no—Software debug messages are discarded. This is the default value.
- yes—Software debug messages are included with log level debug messages.

**Example** `set software-debug = yes`

**Location** LOG

## software-level

**Description** Read-only. Indicates the software-version level of the control module code.

**Usage** The software-level setting is read-only.

**Example** `software-level = H`

**Location** BASE  
SLOT-INFO

**See Also** hardware-level  
software-release  
software-revision  
software-version

## software-release

**Description** Read-only. Displays the engineering or candidate release number of the software image.

**Usage** The software-release setting is read-only.

**Example** `software-release = 9.2-167`

**Location** SLOT-INFO

**See Also** hardware-level  
software-revision  
software-version

## software-revision

**Description** Read-only. Indicates the software revision number of the unit.

**Usage** The software-revision setting is read-only.

**Example** software-revision = 1

**Location** BASE  
SLOT-INFO

**See Also** hardware-level  
software-revision  
software-version

## software-version

**Description** Read-only. Indicates the software version of the unit.

**Usage** The software-version setting is read-only.

**Example** software-version = 1.0

**Dependencies** You can also use the version command to view the current system software version.

**Location** BASE  
SLOT-INFO

**See Also** hardware-level  
software-release  
software-revision

## sonet-far-end-line-coding-violations

**Description** Read-only. Indicates the number of bit-interleaved parity errors at the far-end device's Line layer. A Synchronous Optical Network (SONET) line consists of one or more sections.

**Usage** The sonet-far-end-line-coding-violations value is read-only.

**Example** sonet-far-end-line-coding-violations = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

## sonet-far-end-line-errored-seconds

**Description** Read-only. Indicates the number of errored seconds at the far-end device's Line layer. A Synchronous Optical Network (SONET) line consists of one or more sections.

**Usage** The sonet-far-end-line-errored-seconds value is read-only.



**Example** sonet-far-end-line-errored-seconds = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-far-end-line-severely-errored-seconds

**Description** Read-only. Indicates the number of severely errored seconds at the far-end device's Line layer. A Synchronous Optical Network (SONET) line consists of one or more sections.

**Usage** The sonet-far-end-line-severely-errored-seconds value is read-only.

**Example** sonet-far-end-line-severely-errored-seconds = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-far-end-line-unavailable-seconds

**Description** Read-only. Indicates the number of unavailable seconds at the far-end device's line layer. A Synchronous Optical Network (SONET) line consists of one or more sections.

**Usage** The sonet-far-end-line-unavailable-seconds value is read-only.

**Example** sonet-far-end-line-unavailable-seconds = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-far-end-path-coding-violations

**Description** Read-only. Pertains to Synchronous Optical Network (SONET). Indicates the number of bit-interleaved parity errors at the far-end device's Path layer. A path is an end-to-end circuit.

**Usage** The sonet-far-end-path-coding-violations value is read-only.

**Example** sonet-far-end-path-coding-violations = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-far-end-path-errored-seconds

**Description** Read-only. Pertains to Synchronous Optical Network (SONET). Indicates the number of errored seconds at the far-end device's Path layer. A path is an end-to-end circuit.

**Usage** The sonet-far-end-path-errored-seconds value is read-only.

**Example** sonet-far-end-path-errored-seconds = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-far-end-path-severely-errored-seconds

**Description** Read-only. Pertains to Synchronous Optical Network (SONET). Indicates the number of severely errored seconds at the far-end device's path layer. A path is an end-to-end circuit.

**Usage** The sonet-far-end-path-severely-errored-seconds value is read-only.

**Example** sonet-far-end-path-severely-errored-seconds = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-far-end-path-unavailable-seconds

**Description** Read-only. Pertains to Synchronous Optical Network (SONET). Indicates the number of unavailable seconds at the far-end device's Path layer. A path is an end-to-end circuit.

**Usage** The sonet-far-end-path-unavailable-seconds value is read-only.

**Example** sonet-far-end-path-unavailable-seconds = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-line-coding-violations

**Description** Read-only. Indicates the number of bit-interleaved parity errors at the unit's line layer. A Synchronous Optical Network (SONET) line consists of one or more sections.

**Usage** The sonet-line-coding-violations value is read-only.

**Example** sonet-line-coding-violations = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-line-errored-seconds

**Description** Read-only. Indicates the number of errored seconds at the unit's line layer. A Synchronous Optical Network (SONET) line consists of one or more sections.

**Usage** The sonet-line-errored-seconds value is read-only.

**Example** sonet-line-errored-seconds = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-line-severely-errored-seconds

**Description** Read-only. Indicates the number of severely errored seconds at the unit's line layer. A Synchronous Optical Network (SONET) line consists of one or more sections.

**Usage** The sonet-line-severely-errored-seconds value is read-only.

**Example** sonet-line-severely-errored-seconds = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-line-unavailable-seconds

**Description** Read-only. Indicates the number of unavailable seconds at the unit's line layer. A Synchronous Optical Network (SONET) line consists of one or more sections.

**Usage** The sonet-line-unavailable-seconds value is read-only.

**Example** sonet-line-unavailable-seconds = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-path-coding-violations

**Description** Read-only. Pertains to Synchronous Optical Network (SONET). Indicates the number of bit-interleaved parity errors at the unit's path layer. A path is an end-to-end circuit.

**Usage** The sonet-path-coding-violations value is read-only.

**Example** sonet-path-coding-violations = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-path-errored-seconds

**Description** Read-only. Pertains to Synchronous Optical Network (SONET). Indicates the number of errored seconds at the unit's path layer. A path is an end-to-end circuit.

**Usage** The sonet-path-errored-seconds value is read-only.

**Example** sonet-path-errored-seconds = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-path-severely-errored-seconds

**Description** Read-only. Pertains to Synchronous Optical Network (SONET). Indicates the number of severely errored seconds at the unit's path layer. A path is an end-to-end circuit.

**Usage** The sonet-path-severely-errored-seconds value is read-only.

**Example** sonet-path-severely-errored-seconds = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-path-unavailable-seconds

**Description** Read-only. Pertains to Synchronous Optical Network (SONET). Indicates the number of unavailable seconds at the unit's path layer. A path is an end-to-end circuit.

**Usage** The sonet-path-unavailable-seconds value is read-only.

**Example** sonet-path-unavailable-seconds = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-section-coding-violations

**Description** Read-only. Indicates the number of bit-interleaved parity errors at the unit's section layer. A Synchronous Optical Network (SONET) section is a single run of cable. Section-terminating equipment is any adjacent pair of switches.

**Usage** The sonet-section-coding-violations value is read-only.

**Example** sonet-section-coding-violations = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-section-errored-seconds

**Description** Read-only. Indicates the number of errored seconds at the unit's section layer. A Synchronous Optical Network (SONET) section is a single run of cable. Section-terminating equipment is any adjacent pair of switches.

**Usage** The sonet-section-errored-seconds value is read-only.

**Example** sonet-section-errored-seconds = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-section-severely-errored-framing-seconds

**Description** Read-only. Pertains to Synchronous Optical Network (SONET). Indicates the number of severely errored framing seconds at the unit's section layer. A SONET section is a single run of cable. Section-terminating equipment is any adjacent pair of switches.

**Usage** The sonet-section-severely-errored-framing-seconds value is read-only.

**Example** sonet-section-severely-errored-framing-seconds = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### sonet-section-severely-errored-seconds

**Description** Read-only. Indicates the number of severely errored seconds at the unit's section layer. A Synchronous Optical Network (SONET) section is a single run of cable. Section-terminating equipment is any adjacent pair of switches.

**Usage** The sonet-section-severely-errored-seconds value is read-only.

**Example** sonet-section-severely-errored-seconds = 0

**Location** OC3-ATM-STAT:performance-monitoring  
OC3-ATM-STAT:interval-performance-monitoring

### source-address

**Description** Specifies an IP address. After applying the source-address-mask value, the filter compares the result to the source address in a packet.

**Usage** Specify an IP address. The default is 0.0.0.0, which matches all IP packets.

**Example** set source-address = 2.2.2.2

**Dependencies** This setting applies only if the type parameter in the input-filter or output-filter subprofile is set to ip-filter, route-filter, or tos-filter.

**Location** FILTER:input-filters [n] :ip-filter  
FILTER:output-filters [n] :ip-filter  
FILTER:input-filters [n] :route-filter  
FILTER:output-filters [n] :route-filter  
FILTER:input-filters [n] :tos-filter  
FILTER:output-filters [n] :tos-filter  
TACL:permit-list [n]

## source-address-mask

**Description** Specifies a mask that a filter applies to the source-address value before comparing that value to the source address of a packet. You can use this value to hide the host portion of an address, or its host and subnet portion.

After translating the mask and address into binary format, the system applies the mask to the address by performing a logical AND operation. The mask hides the portion of the address that appears behind each binary 0 (zero) in the mask.

**Usage** Specify a mask in decimal notation.

- The default is 0.0.0.0, which masks all bits.
- A mask of all ones (255.255.255.255) masks no bits, so the system compares the full destination address of a single host.

**Example** set source-address-mask = 255.255.255.224

**Dependencies** This setting applies only if the type parameter in the input-filter or output-filter subprofile is set to ip-filter, route-filter, or tos-filter.

**Location** FILTER:input-filters [n] :ip-filter  
FILTER:output-filters [n] :ip-filter  
FILTER:input-filters [n] :route-filter  
FILTER:output-filters [n] :route-filter  
FILTER:input-filters [n] :tos-filter  
FILTER:output-filters [n] :tos-filter  
TACL:permit-list [n]

## source-if

**Description** Name of the configured soft IP interface whose IP address will be the local address for this connection.

**Usage** The name uses the format sipN, where N is the logical-item value of the soft interface's ip-interface profile. The default value is null.

**Example** set source-if = sip1

**Dependencies** The source-if and local-address parameters cannot both be set in the same profile.

**Location** CONNECTION/"" :ip-options

## source-ip-address

**Description** Source IP address.

**Usage** IP address. After applying the `source-ip-netmask` to this value, a comparison is done. The default value is 0.0.0.0/0.

**Example** `set source-ip-address = 192.168.0.5`

**Dependencies** If the source address of the packet does not match the `source-ip-netmask` of the rule, the comparison fails.

**Location** `PACKET-FLOWS/":flow[n] :packet-classifier`

## source-ip-check

**Description** Enables or disables level 1 antispoofing protection.

**Usage** Valid values are as follows:

- `yes`—Specifies that the system checks all packets received on the interface to ensure that their source IP address matches the combination of address and subnet mask specified by the `remote-address` value, or the address agreed upon in IPCP negotiation.
  - If `remote-address` specifies a subnet, packets that originate on that subnet are accepted.
  - If `remote-address` specifies a 32-bit mask, only packets from that host are accepted.
  - Packets sent from an address that does not match are discarded.
- `no` (the default)—Specifies that antispoofing for the session is disabled.

**Example** `set source-ip-check = yes`

**Dependencies** This setting and the `reverse-path-check` setting are mutually exclusive. Only one of these fields can be enabled in a profile.

**Location** `CONNECTION:ip-options`

**See Also** `ip-address`

## source-ip-netmask

**Description** Mask to be applied to the `source-ip-address` value before a comparison is done.

**Usage** IP address. The default value is 0.0.0.0.

**Example** `set source-ip-netmask = 255.255.255.255`

**Dependencies** If the source address of the packet does not match the `source-ip-address` of the rule, the comparison fails.

**Location** `PACKET-FLOWS/":flow[n] :packet-classifier`

## source-mac-address

**Description** A source MAC address.

**Usage** A six-byte hexadecimal number uniquely representing the source host. The system will forward or discard packets from this address, depending on how the filter is defined.

**Example** `set source-mac-address = 12:34:56:78:9a:bc`

**Location** `FILTER:input-filters[n]:ethernet-filter`

## source-port

### Description

- In the hop-level profile, specifies the physical address of the line interface module (LIM) slot or the trunk port from which data is permitted into the specified queue.
- In the packet-classifier profile, the number to be compared to the source port of a packet when `ip-protocol` has been set to 17 (UDP) or 6 (TCP).

### Usage

- In the hop-level profile, specify the physical address using `shelf`, `slot`, and `port`. The wild-card address `{any-shelf any-slot 0}` indicates that data from any port and LIM slot is permitted into this queue.
- In the packet-classifier profile, if a nonzero `source-port` is specified in a `packet-flow` profile, the `ip-protocol` value must be set to either 17 (UDP) or 6 (TCP). TCP and UDP port numbers are typically assigned to services. For a list of well-known port assignments, see RFC 1700, *Assigned Numbers*. The default value is 0.

### Example

In the hop-level profile, set `source-port = { shelf-1 trunk-module-2 2 }`

In the packet-classifier profile, set `source-port = 6`

**Dependencies** In the packet-classifier profile, if the source address of the packet does not compare as specified to the `source-port` of the rule, the comparison fails.

**Location** `SWITCH-CONFIG:atm-parameters:outgoing-queue`

**See Also** `hop-level`

`PACKET-FLOWS/":flow[n]:packet-classifier`



## source-port-comparison

**Description** Operator to use in the source-port comparison.

**Usage** The following operators can be used to compare source port values:

- none (no comparison is made)
- equal (equal to)
- less (less than)
- greater (greater than)

The default value is none.

**Example** `set source-port-comparison = less`

**Location** `PACKET-FLOWS/"":flow[n]:packet-classifier`

## spared-slot-number

**Description** Read-only. Indicates the primary line interface module (LIM) associated with the spare LIM specified by spare-slot-number parameter.

**Usage** The spared-slot-number value is read-only.

**Example** `spared-slot-number = 2`

**Location** `LIM-SPARING-STATUS`

**See Also** manually-spared-slot-number  
sparing-mode

## spare-physical-address

**Description** Specifies or identifies, depending on the profile, the location of a physical interface or module within the Stinger unit that is acting as a spare. The address has the format {shelf slot item}. The elements of the address are identified as follows:

- shelf—Currently, in Stinger units, the shelf number is always 1.
- slot—Number of the slot in which the module resides.
- item—Number of the interface on the module. Interfaces are numbered starting with 1 for the topmost or leftmost interface on the module. An item number of 0 (zero) denotes the entire slot.

**Usage** Valid values are as follows:

- In the ds1-atm, ds3-atm, e3-atm or oc3-atm profile, specify a complex value that includes the shelf number, slot number and item (port) number of the spare trunk port. If the current port is the primary trunk port, the value identifies its spare (secondary) trunk port. If the current port is the secondary trunk, the value identifies the primary trunk port.

To specify the values, include both spare-physical-address and the relevant subfield in each set command.

- In the al-dmt-stat, ds1-atm-stat, d3-atm-stat, e3-atm-stat, hds12-stat, oc3-atm-stat, shdsl-stat and the shdsl-stat profiles, the spare-physical-address value is read-only.

**Example** To set item 1 on the module in slot 18 as a backup interface:

```
admin> set spare-physical-address shelf = 1
admin> set spare-physical-address slot = 18
admin> set spare-physical-address item-number = 1
```

**Dependencies** In the ds1-atm, ds3-atm, e3-atm, or oc3-atm profile, sparing-state must be set to yes for spare-physical-address to apply.

**Location** AL-DMT-STAT

DS1-ATM-STAT

DS3-ATM:line-config

E3-ATM

HDSL2-STAT

OC3-ATM

SDSL-STAT

SHDSL-STAT

**See Also** sparing-state

## spare-slot-number

**Description** Specifies or indicates the slot number containing the spare link interface module (LIM) and path selector module (PSM) or copper loop test (CLT) module.

**Usage** Valid values are as follows:

- In the lim-sparing-config profile, specify an integer. The default is any-slot. The slot you specify must have a special backup LIM.
- In the lim-sparing-status profile, the spare-slot-number value is read-only. This value is automatically set by the software when the Stinger unit powers up.

**Example** set spare-slot-number = 1

**Dependencies** spare-slot-number does not apply if sparing-mode is set to inactive.

**Location** LIM-SPARING-CONFIG

LIM-SPARING-STATUS

**See Also** manually-spared-slot-number  
spare-physical-address

## spare-slot-type

**Description** Type of spare line interface module (LIM) installed in the slot.

For example, suppose a Stinger unit is configured with an asymmetric digital subscriber line (ADSL) LIM in slot 1 and a symmetric digital subscriber line (SDSL) LIM in slot 4. Slot 14 contains a spare SDSL LIM with a path selector module (PSM), and slot 16 contains a spare ADSL LIM also with a PSM.

**Usage** The default is none. This value is automatically detected and set by the software when the Stinger unit powers up.

**Example** spare-slot-type = none

**Location** LIM-SPARING-CONFIG  
LIM-SPARING-STATUS

**See Also** manually-spared-slot-number  
spare-physical-address

## sparing-change-counter

**Description** Read-only. Displays a count of each redundancy change, including primary to secondary, secondary to primary, and so on.

**Usage** The counter is reset on power-up of the Stinger unit.

**Example** sparing-change-counter = 3

**Location** DS1-ATM-STAT  
DS3-ATM-STAT  
E3-ATM-STAT  
OC3-ATM-STAT  
LIM-SPARING-STATUS  
AL-DMT-STAT  
HDSDL2-STAT  
SDSL-STAT  
SHDSL-STAT

## sparing-change-reason

**Description** Read-only. Indicates how the redundancy setup has been activated.

**Usage** Valid read only values are as follows:

- inactive—Redundancy is not currently activated on this line interface module (LIM).
- manual—The redundancy setup has been manually activated.
- automatic—The redundancy setup has been automatically configured.

**Example** `sparing-change-reason = manual`

**Location** DS1-ATM-STAT  
DS3-ATM-STAT  
E3-ATM-STAT  
OC3-ATM-STAT  
LIM-SPARING-STATUS  
AL-DMT-STAT  
HDSL2-STAT  
SDSL-STAT  
SHDSL-STAT

## sparing-change-time

**Description** Read-only. Indicates the time that the last change in the redundancy state occurred.

**Usage** The `sparing-change-time` value is a read-only display set by the system.

**Example** `sparing-change-time = 0`

**Location** DS1-ATM-STAT  
DS3-ATM-STAT  
E3-ATM-STAT  
OC3-ATM-STAT  
LIM-SPARING-STATUS  
AL-DMT-STAT  
HDSL2-STAT  
SDSL-STAT  
SHDSL-STAT

## sparing-mode

**Description** Enables or disables line interface module (LIM) redundancy, and specifies the redundancy mode to use.

**Usage** Valid values are as follows:

- `manual`—Enables LIM redundancy by deactivating a LIM and terminating its connections, and then reactivating the connections on the spare LIM.
- `inactive`—Disables the LIM redundancy function. This is the default.
- `automatic`—Allows automatic redundancy to be activated according to the values of the parameters in the `lim-sparing-config:auto-lim-sparing-config` subprofile.

**Example** `set sparing-mode = manual`

**Location** DS1-ATM

DS3-ATM

E3-ATM

AL-DMT

HDSDL2

IDSL

LIM-SPARING-CONFIG

LIM-SPARING-STATUS

OC3-ATM

SDSL

SHDSL

## sparing-state

**Description** State of the redundancy function. Specifies or indicates, depending upon the profile in which it occurs, whether the redundancy function for the port is enabled or disabled.

**Usage** Valid values are as follows:

- `sparing-none`—Redundancy is not enabled. This is the default.
- `primary-active`—Redundancy is enabled, and the line interface module (LIM) slot is the primary (spare) LIM.
- `primary-inactive`—Redundancy is not enabled, and the LIM slot is the primary (spare) LIM.
- `secondary-active`—Redundancy is enabled, and the LIM slot is the secondary (spare) LIM, and the spare is inactive.
- `secondary-inactive`—Redundancy is enabled, and the LIM slot is the secondary (spare) LIM, and the spare is active
- `not-applicable`—Indicates that LIM redundancy is not applicable to this module.



**Note** In the `ds3-atm-stat` and `oc3-atm-stat` profiles, the `sparing-state` value is read-only.

**Example** `sparing-state = sparing-none`

**Location** DS1-ATM-STAT

DS3-ATM-STAT

E3-ATM-STAT

OC3-ATM-STAT

LIM-SPARING-STATUS

AL-DMT-STAT

HDSDL2-STAT

SDSL-STAT

SHDSL-STAT



## spvc-retry-interval

**Description** Specifies the number of seconds to wait before reattempting to establish the switched permanent virtual channel (SPVC) after a failed call attempt.

**Usage** The valid range is from 0 (zero) to 3600, with a default of 10 seconds. A 0 (zero) value indicates no retries.

**Example** `set spvc-retry-interval = 10`

**Location** CONNECTION:atm-options  
CONNECTION:atm-connect-options

## spvc-retry-limit

**Description** Specifies the maximum number of consecutive failed call-setup attempts allowed.

**Usage** The default 0 (zero) value indicates no limit, so that the attempts continue until the setup is successful. If you specify a nonzero value and the limit is reached, a management action such as a switched permanent virtual channel (SPVC) restart via Simple Network Management Protocol (SNMP) is required to reinitiate call setup attempts.

**Example** `set spvc-retry-limit = 0`

**Location** CONNECTION:atm-options  
CONNECTION:atm-connect-options

## spvc-retry-threshold

**Description** Specifies the number of consecutive failed call-setup attempts allowed before the system increments its count of switched permanent virtual channel (SPVC) call failures, which can cause an alarm.

**Usage** The valid range is from 0 to 65535, with a default of 1 failed call. A zero value specifies an infinite number of call attempts, which disables alarms for the SPVC.

**Example** `set spvc-retry-threshold = 1`

**Location** CONNECTION:atm-options  
CONNECTION:atm-connect-options

## spvc-target-cac-fail-trap-enabled

**Description** Enables/disables the Stinger unit from sending traps for soft permanent virtual circuit (SPVC) target call failures.

**Usage** Valid values are as follows:

- yes (the default)—Enables sending traps.
- no—Disables sending traps.

**Example** `set spvc-target-cac-fail-trap-enabled = no`

**Location** TRAP

## src-port-cmp

**Description** Specifies whether a filter tests for source port numbers that are equal to a specified `source-port` value, or port numbers that are less than, greater than, or not equal to the specified value.

**Usage** Valid values are as follows:

- `none` (the default)—Does not compare source port numbers.
- `less`—Matches source port numbers less than the `source-port` value.
- `eq1`—Matches source port numbers equal to the `source-port` value.
- `gtr`—Matches source port numbers greater than the `source-port` value.
- `neq`—Matches source port numbers not equal to the `source-port` value.

**Example** `set src-port-cmp = eq1`

**Dependencies** This setting applies only if the `type` parameter in the `input-filter` or `output-filter` subprofile is set to `ip-filter` or `tos-filter`.

**Location** `FILTER:input-filters[n]:ip-filter`  
`FILTER:output-filters[n]:ip-filter`  
`FILTER:input-filters[n]:tos-filter`  
`FILTER:output-filters[n]:tos-filter`

## stack-trace[n]

**Description** Read-only. Indicates the stack trace record created when an error occurred.

**Usage** The `stack-trace` setting is read-only. It consists of an array of six elements.

**Example** `stack-trace = [ 000000 ]`

**Location** ERROR

## standby-upstream-bandwidth-on-trunks

**Description** *Not currently used.* Read-only. Indicates the total bandwidth of all standby trunks.

**Usage** The `standby-upstream-bandwidth-on-trunks` value is read-only.

**Example** `standby-upstream-bandwidth-on-trunks = 466620`

**Location** BANDWIDTH-STATS

**See Also** `Active-Upstream-Bandwidth-On-Trunks`, `max-upstream-bandwidth`



## start-port

**Description** First port to be isolated during an isolation or multiport tone test.

**Usage** Specify a port number between 1 and 72.

**Example** `set start-port = 3`

**Dependencies** This parameter is valid only if `specific-port = no`.

**Location** `LINE-TESTS`

## start-with-menus

**Description** *Not used.*

**Location** `TERMINAL-SERVER:menu-mode-options`

## state

**Description** Specifies or indicates a state, as follows:

- For the `pnni-summary-addr` profile, specifies the current state of advertising the summary address into the peer group.
- For the `redundancy-stats:context-stats` profile, the current state of the controller in this context.

**Usage** Valid values are as follows:

- In the `pnni-summary-addr` profile, specify one of the following values:
  - `advertising`—The summary address is being advertised into the peer group.
  - `suppressing`—The advertisement is currently suppressed.
  - `inactive` (the default)—This summary entry is inactive.
- In the `context-stats` profile, `state` is a read-only parameter with the following possible values:
  - `initial`
  - `load-context`
  - `start-post`
  - `local-post`
  - `remote-post`
  - `selecting`
  - `selection-complete`
  - `inauguration`
  - `primary-to-operational`
  - `loading`
  - `secondary-to-operational`
  - `monitoring`
  - `dead`

**Example** `state = selecting`

**Location** `PNNI-SUMMARY-ADDR`  
`REDUNDANCY-STATS:context-stats`

## `static-pref`

**Description** Specifies the default preference given to static IP routes.

**Usage** Specify a number from 0 to 255. A value of 255 prevents the use of the route. Following are the default preferences for different types of routes:

- 0 (zero)—Connected routes
- 10—Open Shortest Path First (OSPF) routes
- 30—Routes learned from Internet Control Message Protocol (ICMP) redirects
- 100—Routes learned from RIP
- 100—Static routes
- 100—Ascend Tunnel Management Protocol (ATMP) routes

**Example** `set static-pref = 50`

**Location** `IP-GLOBAL`

## `station`

**Description** Specifies or indicates, according to the profile, the following name:

- In a connection profile, `station` specifies the name of the customer premises equipment (CPE) or remote device on the inbound side of the circuit.
- In a soft permanent virtual circuit (SPVC) connection profile, `station` specifies the name of the CPE device followed by a number such as `ray-dsl-1`.
- In the `admin-state-perm-if` profile, `station` indicates the name of a dedicated (nailed-up) or frame relay connection indicated by a connection profile or RADIUS user profile.

**Usage** Valid values are as follows:

- In a connection profile, specify the name of the remote station. You can enter up to 31 characters. The value you specify is case sensitive, and must exactly match the name of the remote device. If you are not sure about the exact name, contact the administrator of the remote network. The default is null.
- In the `admin-state-perm-if` profile, the `station` setting is read-only.

**Example** `set station = robin-gw`

**Dependencies** The name you specify for `station` is not necessarily a Domain Name System (DNS) hostname. The Stinger unit does not use the `station` name to obtain an IP address.

**Location** `ADMIN-STATE-PERM-IF`  
`CONNECTION`

## status-change-trap-enable

**Description** Specifies whether the Stinger unit generates an SNMP trap (notification) when a T1 line changes state.

**Usage** Specify yes or no. The yes value specifies that the unit generates the trap. The no value (the default) specifies that the unit does not generate the trap.

- no—A trap is not generated when a T1 line changes state.
- yes—A trap is generated when a T1 line changes state.

**Example** `set status-change-trap-enable = no`

**Location** T1:line-interface  
DS1-ATM:line-interface

## status-length

**Description** Specifies the number of lines displayed in the status window, including dividing lines. (For a new value to take effect, the user must log in again.)

**Usage** Specify a number from 18 to 993. The default is 18 lines.

**Example** `set status-length = 60`

**Dependencies** The status-length parameter must be less than screen-length parameter by at least six lines.

**Location** USER

**See Also** left-status  
screen-length  
top-status

## stngr-32-idsl

**Description** *Deprecated and not used.*

**Location** LOAD-SELECT

## stur-loop-attenuation

**Description** Read-only. Indicates the current signal reduction in the loop, in decibels. The stur-loop-attenuation value is received by the central office equipment (COE) from the customer premises equipment (CPE), and thus characterizes how the loop attenuation looks from the CPE's perspective.

**Usage** The stur-loop-attenuation setting is read-only.

**Example** `stur-loop-attenuation = 2`

**Location** SHDSL-STAT:physical-statistic

## stur-snr

**Description** Read-only. Indicates the signal-to-noise ratio on the line, in decibels, as reported by the customer premises equipment (CPE) to the central office equipment (COE).

**Usage** The `stur-snr` setting is read-only.

**Example** `stur-snr = 40`

**Dependencies** An `stur-snr` value of 24dB or higher is required for reliable data transfer. The `stur-snr` value is received by reported message from the CPE, as the result of a direct request from the COE. It reflects the CPE's `snr` value.

**Location** `SHDSL-STAT:physical-statistic`

## sub-channel

**Description** Specifies which subchannel to associate with this quality of service (QoS) type. This parameter is effective only with ADSL line interface modules (LIMs) that support dual latency.

**Usage** Valid values are as follows:

- 1—When an ADSL LIM is set to dual-latency, the channel is the fast channel. When dual latency is not used, this value is always used.
- 2—When an ADSL LIM is set to dual-latency, the channel is the interleave channel.

**Example** `set sub-channel = 2`

**Dependencies** The `line-latency-down` and/or `line-latency-up` parameter in the `al-dmt:line-config` subprofile must be set to both for both subchannel values to be effective.

**Location** `ATM-QOS`

## sub-persistence

**Description** Specifies the number of seconds that average line utilization (ALU) must persist below the `target-utilization` threshold before the Stinger unit subtracts bandwidth from the connection.

When subtracting bandwidth, the unit removes the number of channels specified by `decrement-channel-count`. However, it does not clear the base channel of the call, nor does it cause the number of channels to fall below the `minimum-channels` value.

**Usage** Specify an integer from 1 to 300. The default is 10.

**Example** `set sub-persistence = 15`

**Dependencies** The `sub-persistence` parameter has little effect when the `seconds-history` value is high.

**Location** ANSWER-DEFAULT:ppp-answer  
CONNECTION STATION:ppp-options

## subsc-atm-address

**Description** *Not currently used.* Specifies the switched virtual circuit (SVC) prefix used on the user-network interface (not currently supported) to specify the ATM address prefix to the end system across the interface.

**Location** ATM-IF-CONFIG:base-config

## substitute-recv-name

**Description** Specifies the name expected from the far end during bidirectional Challenge Handshake Authentication Protocol (CHAP) authentication, if it is different from the `station` name or username of a RADIUS profile.

**Usage** Specify a name of up to 23 characters. The default is null. Bidirectional authentication requires that the name of the device be checked against a locally defined name. With the default value, the profile name is used.

**Example** `set substitute-recv-name = cpe-test`

**Dependencies** The system does not dial out calls, so this name is used only when a session is using bidirectional CHAP authentication.

**Location** CONNECTION:ppp-options

**See Also** `ppp-options`

## substitute-send-name

**Description** Specifies the name sent to the calling device during bidirectional Challenge Handshake Authentication Protocol (CHAP) authentication, if different from the name specified in the `system` profile. You can specify this name in the `answer-defaults` profile, to affect all bidirectional CHAP authentications, or in a `connection` profile, to supply a name specific to a connection.

**Usage** Specify a name of up to 23 characters. The default is null. Bidirectional authentication requires that the far end checks the name of the called device. With the default value, the system name is used.

**Example** `set substitute-send-name = stinger-auth-name`

**Dependencies** The system does not dial out calls, so this name is used only when a session is using bidirectional CHAP authentication.

**Location** ANSWER-DEFAULTS:ppp-answer  
CONNECTION:ppp-options

**See Also** `ppp-answer`, `ppp-options`

## subtended-connections-enabled

**Description** Indicates whether the subtended connections feature is licensed. This feature allows trunk-to-trunk virtual path (VP) switching on the Stinger trunk aggregation module (TRAM).

**Usage** Valid values are as follows:

- **yes**—Subtended connections feature is licensed.
- **no**—Subtended connections feature is not licensed.

**Example** `subtended-connections-enabled = yes`

**Location** `BASE`

## subtending-hops

**Description** Number of hops (ATM switches) between the subtending Stinger unit and the virtual circuit endpoint. This value is currently supported only for permanent virtual circuits (PVCs) or permanent virtual paths (PVPs).

**Usage** This value is the number of hops a subtended virtual circuit coming into this queue must have. Valid values are as follows:

- **any-level**—A virtual circuit originating any number of hops away is permitted.
- **0-level**—Only a virtual circuit originating less than one hop away is permitted. This is the default.
- **1-level**—Only a virtual circuit originating one hop away is permitted.
- **2-level**—Only a virtual circuit originating two hops away is permitted.
- **3-level**—Only a virtual circuit originating three hops away is permitted.

For PVCs, this value is specified by the user. For soft PVCs (SPVCs), the value is initialized to 1-level.

**Example** `set subtending-hops = 0-level`

**Location** `CONNECTION:atm-qos-options`

**See Also** `atm-qos-options`

## summarize-rip-routes

**Description** Specifies whether to summarize subnet information in RIP-v1 advertisements. If the router summarizes subnet information, it advertises a route to all the subnets in a network of the same class. For example, the route to 200.5.8.13/28 (a class C address) is advertised as a route to 200.5.8.0.

When the virtual router does not summarize information, it advertises each route in its routing table as is.

**Usage** Valid values are as follows:

- **yes**—Summarizes RIP-v1 subnet information.
- **no** (the default)—Advertises each route as it appears in the routing table.

**Example** `set summarize-rip-routes = yes`

**Dependencies** This setting applies only if the `rip` parameter specifies RIP-v1. In a `vrouter` profile, default settings related to RIP are recommended for most sites.

**Location** IP-GLOBAL  
VROUTER

**See Also** `ip-global`  
`vrouter`

## suppress

**Description** Specifies whether the summary address is advertised (propagated into the peer group) or suppressed.

**Usage** Valid values are as follows:

- `true`—The unit suppresses the advertisement of addresses that match the prefix.
- `false` (the default)—Specifies that the summary address is propagated.

**Example** `set suppress = false`

**Location** PNNI-SUMMARY-ADDR

**See Also** `addr-index`, `state` (in `pnni-summary-addr`)

## suppress-host-routes

**Description** Enables or disables suppression of host routes for interfaces with a subnet mask of less than 32 bits. Suppression of host routes occurs as follows:

- If a connection profile includes a subnet mask of less than 32 bits in the `remote-address` setting, host routes for the interface are suppressed while the session is being negotiated. After the session is established, only network routes are advertised for the interface.
- If a connection profile includes a subnet mask of /32 in the `remote-address` setting, host routes for the interface are not suppressed. (Pool addresses also have a 32-bit mask, so they are not suppressed.)

**Usage** Valid values are as follows:

- `yes`—Suppresses host routes.
- `no` (the default)—Advertises host routes.

**Example** `set suppress-host-routes = yes`

**Location** IP-GLOBAL

## suspect-access-resource-enabled

**Description** Specifies whether the suspect-access-resource trap (notification) is enabled.

**Usage** Valid values are as follows:

- yes—Specifies that the suspect-access-resource trap is enabled. This is the default.
- no—Specifies that the suspect-access-resource trap is disabled.

**Example** `set suspect-access-resource-enabled = no`

**Location** TRAP

**See Also** sys-clock-drift-enabled

## sustainable-cell-rate-cells-per-sec

**Description** Indicates the sustainable cell rate (SCR), which is the average cell transmission rate allowed over a given period of time on a given circuit.

**Usage** SCR expressed in cells per second. The default value is 37 CPS, with a valid range from 0 to 353207 CPS. The value of this field is user-writable only if the system profile atm-qos-rate-unit parameter is set to cps.

**Example** `set sustainable-cell-rate-cells-per-sec = 200`

**Location** ATM-QOS

## sustainable-rate-kbits-per-sec

**Description** Indicates the sustainable bit rate in kilobits per second.

**Usage** This setting applies only to variable bit rate (VBR) traffic, for which the bit rate is variable within the values specified for peak cell rate (PCR), sustainable cell rate (SCR), and maximum burst size (MBS). The default value is 16Kbps. The range is from 0 to 149760Kbps. The value of this field is user-writable only if the system profile atm-qos-rate-unit parameter is set to kbps.

**Example** `set sustainable-rate-kbits-per-sec = 32`

**Location** ATM-QOS

## switch-count

**Description** Read-only. Indicates the number of times switchover to the protection channel has occurred in an automatic protection switching (APS) system.

**Usage** The valid range for this read-only parameter is from 0 through 255.

**Example** `switch-count = 32`

**Location** APS-STAT



## switched-call-type

**Description** Specifies the type of bearer-channel capability the Stinger unit sets up for each switched call in a session.

**Usage** Valid values are as follows:

| Values                       | Specifies                                                                                                                                                                                                                                                                                                                           |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| voice                        | The Stinger unit sets up a voice call, even though it will transmit data over the channel. The voice setting assumes that only 56Kbps is available.                                                                                                                                                                                 |
| 56k-restricted (the default) | The Stinger unit sets up a data call with an explicit request for 56Kbps restricted data transfer. Data is transmitted to meet the density requirements for AMI-encoded T1 lines. These requirements dictate that you cannot transmit 16 consecutive zeroes. Use this setting only for a connection that uses robbed-bit signaling. |
| 56k-clear                    | The Stinger unit sets up a data call that uses 56Kbps of the data channel. 56K-Clear is a common setting for T1 PRI lines.                                                                                                                                                                                                          |
| 64k-restricted               | The Stinger unit sets up a data call with an explicit request for 64Kbps restricted data transfer. The call must be set up as a data call at a rate of 64Kbps on an AMI-encoded line. With each transmission, a binary 1 is inserted in the least significant bit position.                                                         |
| 64k-clear                    | The Stinger unit sets up a data call that uses the full 64Kbps bandwidth of the data channel.                                                                                                                                                                                                                                       |
| 144k-clear                   | The Stinger unit sets up a data call that utilizes the full 144Kbps of combined 2B+D data channels.                                                                                                                                                                                                                                 |
| 384k-restricted              | The Stinger unit sets up a data call that connects to Multi-Rate or GlobanD data services at 384Kbps.                                                                                                                                                                                                                               |
| 384k-clear                   | The Stinger unit sets up a data call that connects to the Switched-384 data service. This AT&T data service does not require Multi-Rate or GlobanD.                                                                                                                                                                                 |
| dws-384-clear                | A 384Kbps call coded as Multi-Rate, not H0.                                                                                                                                                                                                                                                                                         |
| 1536k-clear                  | The Stinger unit sets up a data call that connects to the Switched-1536 data service at 1536Kbps. NFAS signaling is required for the Switched-1536 data service. (Because all 24 channels of the T1 PRI line carry user data, the D channel must be on another line.)                                                               |
| 1536k-restricted             | The same service as 1536K-Clear, but with a request for restricted data transfer. With each transmission, a binary 1 is inserted in the least significant bit position.                                                                                                                                                             |

**Values**

128k-clear to 1472k-clear  
(in multiples of 64)  
modem

**Specifies**

Multi-Rate bit rates.

The Stinger unit sets up the call as a voice call.  
When the call is enabled, the Stinger unit routes it  
to a digital modem.

To ensure data integrity:

- Use only digital end-to-end connectivity. No analog signals must be present anywhere in the link.
- Make sure that the telephone company is not using any intervening loss plans to economize on voice calls.
- Do not use echo cancellation. The technology designed to remove echoes from analog lines can scramble data in the link.
- Do not make any modifications that can change the data in the link.

**Example** set switched-call-type = 56k-clear

**Dependencies** Consider the following:

- If a dedicated (nailed-up) connection is in use, `switched-call-type` does not apply.
- You must set this parameter for the `userstat` command to display the correct speed setting.

**Location** FRAME-RELAY

**See Also** data-service

switched-enabled

**Description** *Not used.*

**Location** BASE

## switch-name

**Description** Name set by the system to identify which ATM application-specific integrated circuit (ASIC) can be configured in the switch-config profile.

By default, the system always creates a switch-config profile with switch-name set to controller. If one or more trunk aggregation modules (TRAMs) are installed, the system also creates profiles for those modules with switch-name set to tram-17 (a TRAM installed in slot 17) or tram-18 (a TRAM installed in slot 18).

**Usage** Do not modify the profile index names (controller, tram-17, or tram-18) assigned by the system.

**Example** To display the profile index names:

```
admin> dir switch-config
603 08/02/2001 15:04:14 controller
1964 08/02/2001 15:08:22 tram-17
1770 08/02/2001 15:05:37 tram-18
```

**Dependencies** If no TRAMs are installed, only the controller name is valid.

**Location** SWITCH-CONFIG

## sync-analog-profile

**Description** Specifies the connection profile for synchronous framing and analog bearer dialout request.

**Usage** Specify an alphanumeric text string of up to 31 characters. Default value is blank.

**Example** set sync-analog-profile = analog\_name

**Location** TUNNEL-SERVER:dialout-options

## sync-digital-profile

**Description** Specifies the connection profile for synchronous framing and digital bearer dialout request.

**Usage** Specify an alphanumeric text string of up to 31 characters. The default value is blank.

**Example** set sync-digital-profile = digital\_name

**Location** TUNNEL-SERVER:dialout-options

## sys-clock-drift-enabled

**Description** Specifies whether the SNMP clock-drifted trap (notification) is enabled.

**Usage** Valid values are as follows:

- `yes`—Specifies that the SNMP clock-drifted trap is enabled. This is the default.
- `no`—Specifies that the SNMP clock-drifted trap is disabled.

**Example** `set sys-clock-drift-enabled = no`

**Location** `TRAP`

**See Also** `config-change-enabled`

## syslog-enabled

**Description** Enables or disables forwarding of log messages to the UNIX Syslog server.

**Usage** Valid values are as follows:

- `yes`—Specifies forwarding of log messages to the UNIX Syslog server is enabled.
- `no`—Specifies forwarding of log messages to the UNIX Syslog server is disabled. This is the default.

**Example** `set syslog-enabled = yes`

**Dependencies** Syslog is not a Stinger status display, but a facility that sends system status messages to a host computer, known as the Syslog host. (For information about the `syslog` daemon, see the UNIX man pages for `logger(1)`, `syslog(3)`, `syslog.conf(5)`, and `syslogd(8)`.) The Syslog function requires UDP port 514.

**Location** `LOG`

**See Also** `facility`  
`host`

## syslog-format

**Description** Specifies the system log message format to use.

**Usage** Specify one of the following values:

- `tnt`—Syslog message format is MAX TNT® style. This is the default value.
- `max`—Syslog message format is MAX™ style.

**Example** `set syslog-format = max`

**Location** `LOG`

## syslog-level

**Description** Specifies the lowest level of log messages Stinger unit sends to the Syslog server.

**Usage** All levels above the level you indicate will be included in your Syslog messages. For example, if Alert is specified, messages at Emergency level and messages at Alert level will be included. Specify one of the following values:

| Value                                                                   | Lowest-level message indicates                                                                                                                                                                                     |
|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| none                                                                    | The unit does not display log messages.                                                                                                                                                                            |
| emergency                                                               | The unit has an error condition and is unlikely to be operating normally.                                                                                                                                          |
| alert                                                                   | The unit has an error condition but is still operating normally.                                                                                                                                                   |
| critical                                                                | An interface has gone down or a security error has occurred.                                                                                                                                                       |
| error (the default in log)                                              | An error event has occurred.                                                                                                                                                                                       |
| warning                                                                 | An unusual event has occurred, but the unit is otherwise operating normally. For example, this type of message appears when a login attempt has failed because the user entered an incorrect username or password. |
| notice                                                                  | Events of interest in normal operation have occurred (a link going up or down, for example).                                                                                                                       |
| info<br>(the default in<br>LOG:auxiliary-syslog:<br>auxiliary-syslog n) | State and status changes that are commonly not of general interest have occurred.                                                                                                                                  |
| debug                                                                   | Helpful debugging information.                                                                                                                                                                                     |

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.

**Example** `set syslog-level = notice`

**Dependencies** 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.

**Location** LOG  
LOG:auxiliary-syslog:auxiliary-syslog[n]

**See Also** `syslog-enabled`

## system-8k-clock

**Description** Specifies the 8 kilohertz (kHz) clock source for the unit.

**Usage** Valid values are as follows:

- `controller`—Specifies that the clock source is the control module. This is the default..
- `trunk-module`—Specifies that the clock source is the trunk module framer.
- `bits` (building integrated timing supply)—Specifies that the clock source is the T1 framer.
- `ami-8k`—Specifies that the clock source operates in the Annex C system clock for Japan.

**Example** `set system-8k-clock = trunk-module`

**Dependencies** If the unit detects a T1 signal in the BITS input, it prioritizes the clock source list as follows:

- If the `system-8k-clock` parameter is set to `bits`, the priority is set to the highest (1) and the T1 framer is selected regardless of other available clock sources and priorities.
- If the `system-8k-clock` parameter is set to a value other than `bits`, the priority is set as the lowest (3), and the T1 framer is selected as a clock source only if no other clock sources are available.

**Location** `SYSTEM`

## system-created-slave-profile

**Description** Indicates the `watchdog-config` profile is system-created for a Compact Remote shelf.

**Usage** This parameter is read-only. Valid values are as follows:

- `yes` (the default)—The `watchdog-config` profile is system-created.
- `no`—The `watchdog-config` profile is user-created.

**Example** `system-created-slave-profile = yes`

**Location** `watchdog-config`

## system-ip-addr

**Description** Specifies the source address for IP traffic originating from the Stinger unit or from the global virtual router.

To enable the system to fail over smoothly to a redundant control module, you must set the `system-ip-addr` value to the address of the soft IP interface address. This allows the system IP address to be a single, unchanging address that always maps to the current primary control module. The soft IP interface address is always associated with the current primary control module.

The following algorithm determines the source address of packets from the Stinger unit:

- 1 The source address of IP-routing protocol packets is always the local address of the transmitting interface.
- 2 The source address of transmitted Telnet packets in telnet sessions to the unit is the destination address of the originating TCP SYN packet.
- 3 The source address of all other transmitted packets is the system IP address, if the system-ip-addr parameter specifies an IP address, or the local address of the transmitting interface, if system-ip-addr specifies the null address.

Protocols that follow this algorithm include the following:

- TCP: Defender, Rlogin, TACACS+, Telnet
- UDP: ATMP, DNS, RADIUS accounting, RADIUS authentication, SECURID, SNMP, Syslog, TFTP, Traceroute, VTP

If the system-ip-addr address becomes unreachable because of a topology change in the network, you can still initiate a telnet session to any of the unit's IP interface addresses (subject to packet filtering throughout the network).

**Usage** Specify an IP address. The default is 0.0.0.0. For redundant control modules, specifying the soft interface address is recommended.

**Example** set system-ip-addr = 10.2.3.4

**Location** IP-GLOBAL

## system-password

**Description** *Not used.*

**Location** TERMINAL-SERVER:terminal-mode-configuration

## system-rmt-mgmt

**Description** Enables or disables remote management of the Stinger unit across multichannel calls.

**Usage** Valid values are as follows:

- yes (the default)—Specifies that remote management of the Stinger unit across multichannel calls is enabled.
- no—Specifies that remote management of the Stinger unit across multichannel calls is disabled.

**Example** set system-rmt-mgmt = no

**Location** SYSTEM

**See Also** remote-configuration

## T

### t1000

**Description** Specifies whether code images for Stinger T1000 modules are to be stored in flash memory.

**Usage** Valid values are as follows:

- auto—Loads the code image if a T1000 module is installed. Otherwise, the image is not loaded. This is the default.
- load—Loads the code image when one is present in the tar file
- skip—Does not load the code image when one is present in the tar file

**Example** `set t1000 = auto`

**Location** `LOAD-SELECT`

### t301-ms

**Description** Specifies the maximum amount of time (in milliseconds) that the Stinger unit waits for a response after an alert message is sent. The timer is stopped if a Release Complete or Release message is received before a Connect message, and the call is cleared.

**Usage** Specify a value from 1 to 180000. The default value is 180000 (three minutes).

**Example** `set t301-ms = 170000`

**Location** `ATM-IF-SIG-PARAMS [n] :q2931-options`

### t303-ms

**Description** Specifies the maximum amount of time (in milliseconds) that the Stinger unit waits for a response after an alert message is sent. The timer is stopped when a Connect, Call Proceeding, or Release Complete message is received.

**Usage** Specify a value from 500 to 5000. The default value is 4000.

**Example** `set t303-ms = 5000`

**Location** `ATM-IF-SIG-PARAMS [n] :q2931-options`

### t303-num-retries

**Description** Specifies the number of retries for the timer set by the t303-ms parameter. For each retry, the timer resets and waits for a response until the combined specifications of interval and retries expire or the response is received, whichever comes first.

**Usage** Specify a number from 1 to 4. The default value is 1.



**Example** `set t303-num-retries = 3`

**Location** ATM-IF-SIG-PARAMS [n] :q2931-options

#### t306-ms

**Description** Specifies the maximum amount of time (in milliseconds) that the Stinger unit waits for a response after a Release message is sent with progress indicator No. 8 for inband information. The timer is stopped when a Release Complete message is received.

**Usage** The default value is 30000.

**Example** `set t306-ms = 30000`

**Location** ATM-IF-SIG-PARAMS [n] :q2931-options

#### t308-ms

**Description** Specifies the maximum amount of time (in milliseconds) that the Stinger unit waits for a response after a Release message is sent. This timer is also called the *release indication timer*. The timer is started when the Release message is sent and normally is stopped when the Release or Release Complete message is received.

**Usage** Specify a value from 5000 to 50000. The default value is 30000.

**Example** `set t308-ms = 30000`

**Location** ATM-IF-SIG-PARAMS [n] :q2931-options

#### t308-num-retries

**Description** Specifies the number of retries for the timer set by the t308-ms parameter. For each retry, the timer resets and waits for a response until the combined specifications of interval and retries expire or the response is received, whichever comes first

**Usage** Specify a number from 1 to 4. The default is 1.

**Example** `set t308-num replies = 3`

**Location** ATM-IF-SIG-PARAMS [n] :q2931-options

#### t309-ms

**Description** Specifies the maximum amount of time (in milliseconds) that the Stinger unit waits to reconnect Q.SAAL. Signaling ATM adaptation layer (SAAL) resides between the atm layer and the Q.2931 function, providing reliable transport of Q.2931 messages. After the specified time has elapsed, calls are dropped.

**Usage** When this parameter is set to 0 (the default), a default value based an ATM signaling protocol is used. Specify a value from 0 to 200000.

**Example** `set t309-ms = 10000`

**Location** `ATM-IF-SIG-PARAMS [n] :q2931-options`

#### t310-ms

**Description** Specifies the maximum amount of time (in milliseconds) that the Stinger unit waits for a response after a Setup message is received. This timer is also called the *call proceeding timer*.

**Usage** Specify a value from 5000 to 50000. The default value is 10000.

**Example** `set t310-ms = 20000`

**Location** `ATM-IF-SIG-PARAMS [n] :q2931-options`

#### t313-ms

**Description** Specifies the maximum amount of time (in milliseconds) that the Stinger unit waits for a response after a Connect message is sent. This timer is also called the *connect request timer*. The timer is started when the Connect message is sent and is stopped when the Connect Acknowledge message is received.

**Usage** Valid values range from 1000 to 10000. The default value is 30000.

**Example** `set t313-ms = 10000`

**Location** `ATM-IF-SIG-PARAMS [n] :q2931-options`

#### t316-ms

**Description** Specifies the maximum amount of time (in milliseconds) that the Stinger unit waits for a response after a Restart message is sent. This timer is also called the *restart request timer*. The timer is started when the Restart message is sent and is stopped when the Restart Acknowledge message is received.

**Usage** Specify a value from 10000 to 300000. The default value is 120000.

**Example** `set t316-ms = 110000`

**Location** `ATM-IF-SIG-PARAMS [n] :q2931-options`

#### t316-num-retries

**Description** Specifies the number of retries for the timer set by the t316-ms parameter. For each retry, the timer resets and waits for a response until the combined specifications of interval and retries expire or the response is received, whichever comes first.

**Usage** Specify a number from 1 to 4. The default is 1.

**Example** `set t316-num-retries = 3`

**Location** ATM-IF-SIG-PARAMS [n] :q2931-options

#### t317-ms

**Description** Specifies the maximum amount of time (in milliseconds) that the Stinger unit waits before completing the internal clearing following receipt of a Restart message. The timer is stopped when a Restart Acknowledge message is transmitted to the originator.

**Usage** Specify a value from 10000 to 100000. The default value is 60000.

**Example** `set t317-ms = 60000`

**Location** ATM-IF-SIG-PARAMS [n] :q2931-options

#### t322-ms

**Description** Specifies the maximum amount of time (in milliseconds) that the Stinger unit waits for a response after a Status Enq message is sent.

**Usage** Specify a value from 1000 to 10000. The default value is 4000.

**Example** `set t322-ms = 6600`

**Location** ATM-IF-SIG-PARAMS [n] :q2931-options

#### t322-num-retries

**Description** Specifies the number of retries for the timer set by the t322-ms parameter. For each retry, the timer resets and waits for a response until the combined specifications of interval and retries expire or the response is received, whichever comes first.

**Usage** Specify a number from 1 to 4.

**Example** `set t322-num-retries= 3`

**Location** ATM-IF-SIG-PARAMS [n] :q2931-options

#### t331-ms

**Description** Specifies the maximum amount of time (in milliseconds) that the Stinger unit waits before internally clearing call references.

**Usage** Valid values range from 1000 to 10000. The default is 60000.

**Example** `set t331-ms = 40000`

**Location** ATM-IF-SIG-PARAMS [n] :q2931-options

## t331-num-retries

**Description** Specifies the number of retries for the timer set by the t331-ms parameter. For each retry, the timer resets and waits for a response until the combined specifications of interval and retries expire or the response is received, whichever comes first.

**Usage** Specify a number from 1 to 4. The default is 1.

**Example** set t331-num-retries = 3

**Location** ATM-IF-SIG-PARAMS [n] :q2931-options

## t333-ms

**Description** Specifies the maximum amount of time (in milliseconds) that the Stinger unit waits before internally clearing call references.

**Usage** Specify a value from 1000 to 10000. The default is 10000.

**Example** set t333-ms = 2000

**Location** ATM-IF-SIG-PARAMS [n] :q2931-options

## t391-val

**Description** Specifies the setting for the link Integrity Verification polling timer in frame relay.

**Usage** The value must be less than that of t392-val. The default is 10, which specifies that status requests are spaced 10 seconds apart. You can multiply the value by the number of polling cycles specified by n391-val to calculate the interval at which the user network interface data terminal equipment (UNI-DTE) device requests a full status report.

**Example** set t391-val = 2

**Dependencies** If link-type is set to dce, this parameter does not apply.

**Location** FRAME-RELAY

## t392-val

**Description** Specifies the t392-val interval (in seconds) at which Status Enquiry messages are to be received. If the network does not receive a Status Enquiry message within the specified number of seconds, the network records an error.

**Usage** The default value is 15.

**Example** set n392-val = 3

**Dependencies** If link-type is set to dte, this parameter does not apply.

**Location** FRAME-RELAY

#### t397-ms

**Description** Specifies the maximum amount of time (in milliseconds) that the Stinger unit waits before internally clearing call references.

**Usage** Specify a value from 60000 to 240000. The default is 180000

**Example** `set t397-ms = 80000`

**Location** ATM-IF-SIG-PARAMS [n] :q2931-options

#### t398-ms

**Description** Specifies the maximum amount of time (in milliseconds) that the Stinger unit waits for a response to a Drop Party message that was sent.

**Usage** Specify a value from 1000 to 10000. The default value is 4000.

**Example** `set t398-ms = 6000`

**Location** ATM-IF-SIG-PARAMS [n] :q2931-options

#### t399-ms

**Description** Specifies the maximum amount of time (in milliseconds) that the Stinger unit waits for a response to an Add Party message that was sent.

**Usage** Specify a value from 10000 to 20000. The default is 14000.

**Example** `set t399-ms = 16000`

**Location** ATM-IF-SIG-PARAMS [n] :q2931-options

#### table-config[n]

**Description** An array of up to eight elements, each of which defines a hostname-address pair as an entry in the local Domain Name System (DNS) table. If the auto-update parameter is set to yes, the system creates table entries from successful DNS queries.

**Usage** For each element in the array, specify a hostname and an associated IP address. Defaults are null and 0.0.0.0.

**Example** To define the first entry in the local DNS table, list the contents of table-config 1 and then set the parameters, as follows:

```
admin> list table-config 1
[in IP-GLOBAL:dns-local-table:table-config[1]]
host-name = ""
ip-address = 0.0.0.0
admin> set host-name = boffin
admin> set ip-address = 10.0.0.1
```

**Dependencies** The auto-update parameter must be set to `yes` for the system to create table entries from successful DNS queries.

**Location** IP-GLOBAL:dns-local-table

## tacp-tx-cell-count

**Description** Read-only. Pertains to Asynchronous Transfer Mode (ATM). Indicates the Transmit ATM Cell Processor (TACP) transmit cell count.

**Usage** The `tacp-tx-cell-count` value is read-only.

**Example** `tacp-tx-cell-count = 0`

**Location** OC3-ATM-STAT

## tag

**Description** Specifies a link as follows:

- Within the `snmpv3-notification` profile, specifies a value that links the `snmpv3-notification` profile with the `trap` profile specifying the host address to which notification messages are sent.
- Within the `frdlci-stat` profile, specifies a numeric value associated with the data link connection identifier (DLCI) on the owning card.

**Usage** Valid values are as follows:

- For the `snmpv3-notification` profile, specify up to 255 characters. The default is null.
- For the `frdlci-stat` profile, a read only value between 0 and 4294967295.

**Example** `set tag = newtag`

**Location** FRDLCI-STAT  
SNMPV3-NOTIFICATION

## tag-or-discard

**Description** Enables or disables tagging of cells that do not conform to the sustainable cell rate (SCR) part of the traffic contract. Tagging means changing the cell loss priority (CLP) bit to 1. Cells not conforming to program clock reference (PCR) are discarded.

**Usage** Valid values are as follows:

- `tag`—Enables tagging
- `discard`—Disables tagging. This is the default.

**Dependencies** If you set the `traffic-descriptor-type` to `clp-tagging-scr`, `noclp-tagging-noscr`, or `clp-tagging-scr`, this parameter is set to `tag`. If you set the traffic descriptor type to any other value, the `tag-or-discard` parameter is set to `discard` (the default)

**Example** `set tag-or-discard = tag`

**Location** `ATM-QOS`

## target-atm-address

**Description** Specifies the ATM address of the destination port on which the target switch establishes the target permanent virtual circuit (PVC) to the destination end system.

**Usage** The value can be a 40-digit hexadecimal number or an alias that has been defined to represent the number.

**Example** `target-atm-address = 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00+`

**Dependencies** The `target-atm-address` parameter does not apply if the `conn-kind` value is set to `pvc`.

**Location** `CONNECTION:atm-connect-options`

## target-noise-margin-down

**Description** Specifies the downstream noise margin the line must achieve relative to 0dB to initialize successfully and to rate adapt during normal operations.

**Usage** Specify an integer from 1 to 31 representing decibels. The default is 6dB. The line interface module (LIM) limits the maximum noise margin to 15dB. If you specify a setting greater than 15, the LIM uses 15dB.

**Example** `set target-noise-margin-down = 10`

**Location** `AL-DMT:marging-config`

**See Also** `target-noise-margin-up`

## target-noise-margin-up

**Description** Specifies the upstream noise margin the line must achieve relative to 0dB to initialize successfully and to rate adapt during normal operations.

**Usage** Specify an integer from 1 to 31 representing decibels. The default is 6db. The line interface module (LIM) limits the maximum noise margin to 15dB. If you specify a setting greater than 15, the LIM uses 15dB.

**Example** `set target-noise-margin-up = 15`

**Location** `AL-DMT:marging-config`

**See Also** `target-noise-margin-down`

## target-params-name

**Description** Specifies the value indicated by the name setting in the `snmpv3-target-param` profile.

**Usage** Specify up to 22 characters.

**Example** `set target-params-name = profile1`

**Location** TRAP

## target-select

**Description** Specifies the method of assigning the virtual path identifier-virtual channel identifier (VPI-VCI) pair for the target permanent virtual channel (PVC).

**Usage** Valid values are as follows:

- `required`—Specifies that the target switch builds a read-only Connection profile using the VPI-VCI pair specified by the Target-VPI and Target-VCI settings, which are provided by the initiator switch during the signaling setup. This is the default.
- `any`—Specifies that the target switch provides the VPI-VCI pair to the soft PVC (SPVC), and the Target-VPI and Target-VCI settings on the SPVC initiator do not apply.

**Example** `set target-select = required`

**Location** CONNECTION

## target-utilization

**Description** Specifies a number representing the percentage of line utilization to use as a threshold for determining when to add or subtract bandwidth.

The Stinger unit adds bandwidth when average line utilization (ALU) exceeds the target-utilization value, and subtracts bandwidth when it falls below that value for a specified amount of time.

**Usage** Specify a number from 0 to 100. The default is 70.

**Example** `set target-utilization = 70`

**Location** ANSWER-DEFAULTS:mp-answer  
CONNECTION:mp-options

**See Also** `seconds-history`

## target-vci

**Description** Specifies the virtual channel identifier (VCI) for the target permanent virtual channel (PVC), when Target-Select is set to `required`.

**Usage** Specify a number to be assigned to the target PVC. The default value is 0 (zero)



**Example** `set target-vci = 0`

**Location** CONNECTION

**See Also** target-select, target-vpi

## target-vpi

**Description** Specifies the virtual path identifier (VPI) for the target permanent virtual channel (PVC), when target-select is set to required.

**Usage** Specify a number to be assigned to the target PVC. The default value is 0 (zero)

**Example** `set target-vpi = 0`

**Location** CONNECTION

**See Also** target-select, target-vci

## tcc-ms

**Description** Specifies the time (in milliseconds) for control protocol data units (PDU's) (BGN, END, RESYNC).

**Usage** Valid values range from zero (0) to 3000. The default value is 1000.

**Example** `set tcc-ms = 1000`

**Location** ATM-IF-SIG-PARAMS [n] :gsaal-options

**See Also** tidle-ms

## tcp

**Description** *Not used.*

**Location** TERMINAL-SERVER:terminal-mode-configuration

## tcp-estab

**Description** Enables or disables application of the filter only to packets in an established TCP session.

**Usage** Specify yes or no. The default is no.

- yes—Filters only packets that are part of established TCP connections.
- no—Filters packets that are not part of an established TCP connection.

**Example** `set tcp-estab = yes`

**Dependencies** This setting applies only if the `type` parameter in the `input-filter` or `output-filter` subprofile is set to `ip-filter` and `protocol` is set to 6 (TCP).

**Location** `FILTER:input-filters[n]:ip-filter`  
`FILTER:output-filters[n]:ip-filter`

## tcp-syn-flood-protect

**Description** Enables or disables a flush of old Transmission Control Protocol (TCP) sockets that are in a `Tcps_synrcvd` state, when a heavy Tcp-syn flooding occurs.

**Usage** Valid values are as follows:

- `yes`—Enables a flush of these sockets.
- `no`—Disables any flush of these sockets.

**Example** `set tcp-syn-flood-protect = yes`

**Location** `IP-GLOBAL`

## tcp-timeout

**Description** Specifies an interval for TCP retry attempts. After the specified number of seconds elapses, the retries stop and the connection is considered lost.

**Usage** Specify a number of seconds for a TCP time-out. Valid values range from 0 seconds (the default) to 200 seconds.

- With the default value of 0 (zero), the system attempts a fixed number of retries at escalating intervals, adding up to about 170 seconds total.
- If you set `tcp-timeout` to a nonzero value, the value is the number of seconds TCP retries persist. (Other limits in the system terminate TCP retries after about 170 seconds, even if the value is set to a higher number.)

**Example** `set tcp-timeout = 30`

**Location** `IP-GLOBAL`

## tdr-automatic-fault-distance

**Description** Read-only. Indicates the distance to the first detected fault in a copper loop test (CLT). This value is only generated for time domain reflectometry (TDR) tests in automatic mode.

**Usage** Read-only value reported in hundredths (0.01) of a foot for English units or centimeters for metric units.

**Example** `tdr-automatic-fault-distance = 100000`

**Location** `CLT-RESULT`

## tdr-automatic-result

**Description** Read-only. Indicates the distance to the first detected fault in a copper loop test (CLT). This value is only generated for time domain reflectometry (TDR) tests in automatic mode.

**Usage** The TDR-Automatic-Result value is read-only, reported in hundredths (0.01) of a foot for English units or centimeters for metric units.

**Example** `tdr-automatic-result = 0`

**Location** CLT-RESULT

**See Also** `tdr-automatic-result`

## tdr-avg

**Description** Specifies the number of times the time domain reflectometry (TDR) pulse is sent in a copper loop test (CLT).

**Usage** Range is from 1 to 5 pulses. Results are averaged if more than one pulse is used.

**Example** `set tdr-avg = 2`

**Location** CLT-COMMAND

## tdr-distance-level

**Description** Read-only. Indicates TDR-Sample-Count pairs of time domain reflectometry (TDR) test data. The second number in each pair is the level-axis raw data.

**Usage** The `tdr-distance-level` is a read-only value. The first number in each pair is the distance in hundredths (0.01) of a foot for English units or in centimeters for metric units.

**Example** `tdr-distance-level = [ { 0 0 } { 0 0 } { 0 0 } { 0 0 } { 0 0 } { 0+`

**Location** CLT-RESULT

## tdr-gauge

**Description** Specifies the gauge of the cable in the loop in a copper loop test (CLT).

**Usage** Valid values are as follows:

- 22, 24, or 26 AWG if English units are used.
- 4, 5, or 6 tenths of a millimeter if metric units are used.

**Example** `set tdr-gauge = 4`

**Location** CLT-COMMAND

## tdr-get-type

**Description** Specifies the type of time domain reflectometry (TDR) test in a copper loop test (CLT).

**Usage** Valid values are as follows:

- auto—First fault is automatically detected.
- manual—User specifies the measurement range.

**Example** `set tdr-get-type = manual`

**Location** CLT-COMMAND

## tdr-manual-sample-count

**Description** Read-only. Indicates the number of distance or level data points returned for a time domain reflectometry (TDR) test in a copper loop test (CLT).

**Usage** Read-only numeric value. If the TDR test is performed in auto mode and no faults are found, `tdr-manual-sample-count` is set to 0.

**Example** `tdr-manual-sample-count = 0`

**Location** CLT-RESULT

## tdr-measurement-length

**Description** Specifies the total length of a measurement in manual mode starting from the start-distance in a copper loop test (CLT).

**Usage** Specify a number according to the units used:

| If units used are | Specify                                                                                                            |
|-------------------|--------------------------------------------------------------------------------------------------------------------|
| english           | A number from 100 to 20,000 to designate feet. Start-distance plus measurement length must not exceed 20,000 feet. |
| metric            | A number from 32 to 6097 to designate meters. Start-distance plus measurement length must not exceed 6097 meters.  |

**Example** `set tdr-measurement-length = 10000`

**Location** CLT-COMMAND

## tdr-sample-count

**Description** Read-only. Indicates the number of distance or level data points returned for a time domain reflectometry (TDR) test in a copper loop test (CLT).

**Usage** If the TDR test is performed in auto mode and no faults are found, Sample-Count is set to 0.

**Example** `tdr-sample-count = 0`

**Location** `CLT-RESULT`

**See Also** `tdr-automatic-result`

## `tdr-start-distance`

**Description** Specifies the distance at which to start time domain reflectometry (TDR) measurement in manual mode in a copper loop test (CLT).

**Usage** Specify a number according to the units used. The default is 0.

| If units used are | Specify |
|-------------------|---------|
|-------------------|---------|

|                      |                                               |
|----------------------|-----------------------------------------------|
| <code>english</code> | A number from 15 to 20,000 to designate feet. |
|----------------------|-----------------------------------------------|

|                     |                                              |
|---------------------|----------------------------------------------|
| <code>metric</code> | A number from 5 to 6097 to designate meters. |
|---------------------|----------------------------------------------|

**Example** `set tdr-start-distance = 6000`

**Location** `CLT-COMMAND`

## `tdr-unit`

**Description** Specifies the units of measurement for time domain reflectometry (TDR) testing.

**Usage** Valid values are as follows:

- `english`—English units are used for the measurement.
- `metric`—Metric units are used for the measurement. This is the default.

**Example** `set tdr-unit = metric`

**Location** `CLT-COMMAND`

**See Also** `tdr-gauge`

## `tdr-vp`

**Description** Specifies the velocity of propagation for the cable under test in a copper loop test (CLT).

**Usage** The valid range is from 40 to 99 percent of the speed of light. The default value is 0.

**Example** `set tdr-vp = 90`

**Location** `CLT-COMMAND`

**See Also** `tdr-gauge`

## telnet

**Description** *Not used.*

**Location** `TERMINAL-SERVER:terminal-mode-configuration:telnet-options`

## telnet-host-auth

**Description** *Not used.*

**Location** `TERMINAL-SERVER:immediate-mode-options`

## telnet-mode

**Description** *Not used.*

**Location** `TERMINAL-SERVER:terminal-mode-configuration:telnet-options`

## telnet-password

**Description** *Not used.*

**Location** `IP-GLOBAL`

## temporary-route

**Description** Specifies that the Stinger unit adds the route to the routing table only when the link is up. Temporary-Route is especially useful for dedicated (nailed-up) IP-routing connections.

**Usage** Valid values are as follows:

- **yes**—Specifies that a route from the routing table is excluded when its connection is down.
- **no**—Specifies that a route from the routing table is included even if its connection is down. This is the default.

**Example** `set temporary-route = no`

**Location** `CONNECTION:ip-options`

## terminal-type

**Description** *Not used.*

**Location** `TERMINAL-SERVER:terminal-mode-configuration`

## term-rate

**Description** Specifies the bit rate of a Stinger serial port. When you modify the bit rate of a serial port, you might also need to change the data-rate setting of the terminal accessing that port.

**Usage** Specify one of the following values:

57600  
38400  
19200  
9600 (the default)  
4800  
2400

**Example** `set term-rate = 19200`

**Location** SERIAL

## test-iteration-interval

**Description** Specifies the time period in minutes between two tests.

**Usage** Specify a value from 0 through 10000. The default is 30.

**Example** `set test-iteration-interval = 60`

**Location** ATM-OAM:loopback-config

## test-operation

**Description** Specifies the type of copper loop test (CLT).

**Usage** Select one of the following values.

- `dmm-test`—Starts digital multimeter (DMM) tests.
- `line-inls-test`—Starts an insertion loss test.
- `line-bgns-test`—Starts a background noise test.
- `line-signs-test`—Starts a signal-to-noise test.
- `line-lpres-test`—Starts a loop resistance test.
- `line-cldet-test`—Starts a load coil detection test.
- `line-impstart-test`—Starts an impulse noise test.
- `line-impread-test`—Reads the current result of an impulse noise test.
- `line-impstop-test`—Stops an impulse noise test.
- `calib-test`—Calibrates the internal test head.
- `tonesnd-test`—Sends a test tone down the loop.
- `tonercv-test`—Measures the amplitude and frequency of the tone.
- `tldrset-test`—Sets TDR parameters.
- `tldr-get`—Runs a TDR test.
- `cltm-reset-test`—Resets test head electronics.
- `cltm-version`—Reports version numbers of hardware and software.
- `cltm-download`—Downloads CLT module code.
- `dmm-dcdel-test`—Starts DMM dc delta test.
- `dmm-cape-test`—Starts DMM equivalent capacitance test.

- dmm-all-test—Starts DMM ALL test.
- tx-ctrl-tone-test—Sends a control tone.
- tx-trace-tone-test—Sends a trace tone.
- stop-tone-test—Stops sending tones.
- det-ringer-test—Starts a detect ringer test.
- det-atur-test—Starts an ATU-R detection test. ADSL LIMs only.
- btap-test—Starts a bridge tap detection test.
- voice-det-test—Starts a voice signal detection test.
- line-fclloc-test—Starts a first load coil detection test.
- line-shortloc-test—Starts a short-circuit location test.
- set-responder-test—Places CLT module in or out of responder mode.
- set-bypass-test—Toggles splitter bypass.
- splitter-detect-test—Tests for the presence of a splitter.
- dmm-acdel-test—DMM ac delta test.
- dmm-lbal-test—Longitudinal balance test.
- dmm-soak-test—Soak measurement. *Not supported.*
- send-voice-test—Send voice signal.
- meas-voice-test—Voice signal detection.
- meas-dta-test—Analyze subscriber dial tone.
- detaptor-test—Detaptor test.

**Example** set test-operation = line-bgns-test

**Location** CLT-COMMAND

**See Also** test-result-status

## test-result-sequence

**Description** Read-only. Indicates the sequence of the last test result.

**Usage** Read-only number value with a range of 0 to 4294967295.

**Example** test-result-sequence = 9

**Location** CLT-RESULT

## test-result-status

**Description** Read-only. Indicates the status of a copper loop test.

**Usage** Valid values are as follows:

- not-valid—Test has not been performed or is in progress.
- valid—Test is complete and the results are viable in the profile.
- out-of-range—Test failed because of measurements or parameters that were out of range.



**Example** `test-result-status = valid`

**Location** `CLT-RESULT`

## `test-result-time-stamp`

**Description** Read-only. Indicates the number of hours, minutes, and seconds that the system was operational (system uptime) when a test result was obtained.

**Usage** Read-only value with a range of 0 to 4294967295.

**Example** `test-result-time-stamp = 12324`

**Location** `CLT-RESULT`

## `test-sequence`

**Description** Read-only. Indicates the sequence of the last issued test command.

**Usage** Read-only number value with a range of 0 to 4294967295.

**Example** `test-sequence = 9`

**Location** `CLT-COMMAND`

## `test-terminal`

**Description** Specifies which copper loop test (CLT) module or path selector module (PSM) terminal to connect the test tone to.

**Usage** Valid values are as follows:

- `external-tester-terminal` (the default)
- `aux-tester-terminal`

**Example** `set test-terminal = aux-tester-terminal`

**Dependencies** This parameter is only relevant to the `tone-gen` test.

**Location** `LINE-TESTS`

## `test-time-stamp`

**Description** Read-only. Indicates the number of hours, minutes, and seconds that the system was operational (system uptime) when the last test command was issued.

**Usage** Read-only value with a range of 0 to 4294967295.

**Example** `test-time-stamp = 12324`

**Location** `CLT-COMMAND`

## test-type

**Description** Defines the type of line test to be performed.

**Usage** Valid values are as follows:

- gal-iso—Specifies the galvanic isolation test. This is the default.
- tone-gen—Specifies the multiport tone generation test.

**Example** set test-type = tone-gen

**Location** LINE-TESTS

## text-n

**Description** *Not used.*

**Location** TERMINAL-SERVER:menu-mode-options

## time-elapsed

**Description** Read-only. Reports the number of seconds since the start of the current performance measurement interval of the SNMP sonetMediumTimeElapsed field.

**Usage** Read the oc3-atm-stat profile to display the current value for the field.

**Example** time-elapsed = 8

**Location** OC3-ATM-STAT

## third-login-prompt

**Description** *Not used.*

**Location** TERMINAL-SERVER:terminal-mode-configuration

## third-party

**Description** Enables or disables Open Shortest Path First (OSPF) third-party routing for a static route.

**Usage** Valid values are as follows:

- yes—Enables third-party routing for the OSPF router. When third-party is set to yes, the gateway-address value is the third-party router for the route.
- no (the default)—Disables third-party routing for the OSPF router.

**Example** set third-party = yes

**Location** IP-ROUTE

## third-prompt-sequence

**Description** *Not used.*

**Location** `TERMINAL-SERVER:terminal-mode-configuration`

## thresh-profile

**Description** *Not used.* Specifies the name of a DSL-Threshold profile.

**Usage** Specify a name of up to 22 characters. A 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 two profiles.

**Example** `set thresh-profile = dsl-thrprof1`

**Location** `AL-DMT`  
`HDSL2`

## throttle-no-port-match-udp-traffic-on-slot

**Description** Enables or disables reception of UDP packets for UDP ports currently unknown to the Stinger unit. The system discards UDP packets until it receives packets for which the UDP port is known.

**Usage** Specify `yes` or `no`. The default is `no`.

- `yes`—Disable reception of UDP packets for UDP ports unknown to the Stinger unit.
- `no`—Enables reception of UDP packets for UDP ports unknown to the Stinger unit. This is the default.

**Example** `set throttle-no-port-match-udp-traffic-on-slot = no`

**Location** `IP-GLOBAL`

## tidle-ms

**Description** Pertains to the signaling ATM adaptation layer (SAAL) of Asynchronous Transfer Mode (ATM). Specifies the interval (in milliseconds) during which the Q.SAAL layer is idle, for UNI 3.1 only.

**Usage** Valid values range from 1000 to 20000. The default value is 15000.

**Example** `set tidle-ms = 15000`

**Location** `ATM-IF-SIG-PARAMS [n] :qsaal-options`

**See Also** `tcc-ms`

## time-stamp

**Description** Read-only. Indicates the time at which the local node recognized connectivity from the advertising node to the reachable address prefix.

**Usage** The time-stamp setting is read-only.

**Example** time-stamp = 0

**Location** PNNI-ROUTE-ADDR

## tkeepalive-ms

**Description** Pertains to the signaling ATM adaptation layer (SAAL) of Asynchronous Transfer Mode (ATM). Specifies the poll interval (in milliseconds) when the Q.SAAL layer is active in a transient state.

**Usage** When the tkeepalive-ms parameter is set to 0 (the default), a default value based on an ATM signaling protocol is used. Valid values range from 0 to 3000.

**Example** set tkeepalive-ms = 0

**Location** ATM-IF-SIG-PARAMS [n] :qsaal-options

**See Also** tpoll-ms

## tnoresponse-ms

**Description** Specifies the maximum interval (in milliseconds) between receipt of STAT protocol data units (PDUs).

**Usage** When the tnoresponse-ms parameter is set to 0 (the default), a default value based on an Asynchronous Transfer Mode (ATM) signaling protocol is used. Valid values range from 0 to 20000.

**Example** set tnoresponse-ms = 0

**Location** ATM-IF-SIG-PARAMS [n] :qsaal-options

**See Also** tpoll-ms

## tns-advertised-port-id

**Description** Specifies the port ID on the advertising node of the interface used to reach the transit network.

**Usage** Specify a number to assign to the transit network selection (TNS) port ID. The default value is 0.

**Example** set tns-advertised-port-id = 3

**Location** PNNI-ROUTE-TNS

## tns-advertising-node-id

**Description** Specifies the Private Network-to-Network Interface (PNNI) node ID of a node that advertises this route.

**Usage** You can enter the full 22-byte ID or an alias.

**Example** `set tns-advertising-node-id = 00:00:00:00:00:00:00:00:00:00:00:00+`

**Location** PNNI-ROUTE-TNS

## tns-if-index

**Description** Specifies the local interface over which a transit network can be reached.

**Usage** Specify a number to assign to the index. The zero value specifies an unknown interface or reachability through a remote node. This is the default value.

**Example** `set tns-if-index = 0`

**Dependencies** A nonzero value is allowed only if the value of the Tns-Proto parameter is not `pnni`, and the node identified by Tns-Advertising-Node-Id is instantiated within this non-PNNI switching system.

**Location** PNNI-ROUTE-TNS

## tns-metrics-tag

**Description** Specifies a tag representing a group of metric settings that apply to the connectivity from an advertising node to a reachable transit network.

**Usage** The tag must be defined in one or more PNNI-Metrics profiles. If no traffic parameters apply, the zero value is used. This is the default value.

**Example** `set tns-metrics-tag = 0`

**Location** PNNI-ROUTE-TNS

## tns-originate-advertisement

**Description** Specifies whether or not the transit network is advertised by the local node into its Private Network-to-Network Interface (PNNI) routing domain.

**Usage** Valid values are as follows:

- `false`—The local node does not advertise reachability of the transit network.
- `true`—The local node advertises reachability of the transit network. This is the default.

**Example** `set tns-originate-advertisement = false`

**Location** PNNI-ROUTE-TNS

## tns-pnni-scope

**Description** Specifies the extent of the advertisement of reachability from the advertising node to the transit network. *Scope* means the routing range of a connection.

**Usage** Specify a value from 0 to 104. The default value is 0.

**Example** `set tns-pnni-scope = 0`

**Location** PNNI-ROUTE-TNS

## tns-proto

**Description** *Not used.* Specifies the mechanism by which the advertising node learned of reachability to the transit network.

**Usage** Valid values are as follows:

- `other`— Unspecified
- `local`—A local routing protocol such as Integrated Local Management Interface (ILMI).
- `mgmt`—A management protocol such as Simple Network Management Protocol (SNMP).
- `pnni`—ATM Forum Private Network-to-Network Interface (PNNI) dynamic routing protocol.

**Example** `set tns-proto = other`

**Location** PNNI-ROUTE-TNS

## tns-route-type

**Description** Specifies the type of connectivity from the advertising node to the transit network.

**Usage** Valid values are as follows:

- `other` —Unspecified
- `reject`— A route that discards traffic
- `internal`— Directly attached to the logical node advertising the address
- `exterior`—Reachable through the PNNI routing domain, but which is not located in the PNNI routing domain). This is the default.

**Example** `set tns-route-type = internal`

**Location** PNNI-ROUTE-TNS

## tns-vp-capability

**Description** Read-only. Indicates whether virtual path connections (VPCs) can be established from the advertising node to the reachable transit network. Pertains to Private Network-to-Network Interface (PNNI).

**Usage** Valid values are as follows:

- true—VPCs can be established from the advertsing node.
- false—VPCs can not be established from the advertsing node. This is the default value.

**Example** tns-vp-capability = no

**Location** PNNI-ROUTE-TNS

## toggle-screen

**Description** *Not used.*

**Location** TERMINAL-SERVER:menu-mode-options

## tone-send-freq

**Description** Specifies the frequency of a sent tone in a copper loop test.

**Usage** The valid range is from 10kHz to 1600kHz. The default is 0.

**Example** set tone-send-freq = 20

**Location** CLT-COMMAND

## tone-send-level

**Description** Specifies the amplitude of a sent tone in a copper loop test.

**Usage** The valid range is from -10dBm to 10dBm. The default is 0.

**Example** set tone-send-level = 1

**Location** CLT-COMMAND

## tone-send-period

**Description** Specifies the amount of time a tone is sent in a copper loop test.

**Usage** The valid range is from 0 to 20 minutes. The default is 0.

**Example** set tone-send-period = 1

**Location** CLT-COMMAND

## top-high-temperature-threshold

**Description** *Not supported.* Specifies the top control module (CM) thermal sensor high temperature trigger level, in degrees Celsius (C). When the temperature exceeds this value, an alarm or watchdog state can be generated.

**Usage** Specify a numeric value between -20 degrees C and 75 degrees C (-4 degrees F and 167 degrees F). The default is 60 degrees C (140 degrees F).

**Example** `set top-high-temperature-threshold = 65`

**Dependencies** *Not supported.* This threshold can be used for setting an alarm profile and watchdog-config profile trap (notification). Temperature sensors are available only in version 3 and higher of the control module.

**Location** THERMAL

## top-low-temperature-threshold

**Description** *Not supported.* Specifies the top control module (CM) thermal sensor low temperature trigger level (in degrees Celsius). When temperature falls below this value, an alarm or watchdog state can be generated.

**Usage** Specify a numeric value between -20 degrees C and 75 degrees C (-4 degrees F and 167 degrees F). A value of 0 degrees C (32 degrees F) is the default.

**Example** `set top-low-temperature-threshold = 15`

**Dependencies** This threshold can be used for setting an alarm profile and watchdog-config profile trap (notification). Temperature sensors are available only in version 3 and higher of the control module.

**Location** THERMAL

## top-status

**Description** Specifies the default content of the upper-right portion of the status window.

**Usage** Valid values are as follows:

- `general-info`—Specifies that the Stinger unit displays general information and statistics for the system. This is the default.
- `log-window`—Specifies that the Stinger unit displays saved system-event log entries.
- `line-status`—Specifies that the Stinger unit displays the status of system telephony interfaces.

**Example** `set top-status = general-info`

**Location** USER



## tos-filter

**Description** Specifies the name of a filter profile defining a type-of-service (TOS) filter. TOS filters are used to enable proxy-quality-of-service (QoS) handling for packets that match the filter specification.

**Usage** Specify the filter name. The default is null, which indicates no filter.

**Example** `set tos-filter = proxy-qos`

**Location** CONNECTION:ip-options

## total-count

**Description** Read-only. Indicates the total number of a particular class of devices present in the system.

**Usage** The total-count setting is read-only.

**Example** `total-count = 10`

**Location** DEVICE-SUMMARY

## total-loopback-tests

**Description** Specifies the total number of tests to be performed on this interface.

**Usage** 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.

**Example** `set total-loopback-tests = 10`

**Location** ATM-OAM:loopback-config

## tpoll-ms

**Description** Specifies the poll interval (in milliseconds) when the Q.SAAL layer is active.

**Usage** When the tpoll parameter is set to 0 (the default), a default value based on an Asynchronous Transfer Mode (ATM) signaling protocol is used. Valid values range from 0 to 3000.

**Example** `set tpoll-ms = 0`

**Location** ATM-IF-SIG-PARAMS [n]:qsaal-options

**See Also** tkeepalive-ms, tnoresponse-ms

## tpg-state

**Description** Enables or disables the test pattern procedure.

**Usage** Valid values are as follows:

- `disabled`— Test pattern procedure is currently disabled on this link. This is the default.
- `operating`— Test pattern procedure is currently operating on this link

**Example** `set tpg-state = disabled`

**Location** IMAGROUP

**See Also** `tpg-test-link`, `tpg-test-pattern`

## tpg-test-link

**Description** Specifies a Simple Network Management Protocol (SNMP) interface as the test link for use in the test pattern procedure.

**Usage** The valid range is from -1 to 24. The default is zero.

**Example** `set tpg-test-link = -1`

**Location** IMAGROUP

IMA-GROUP-STAT

IMA-GROUP-STAT:ima-rt

**See Also** `tpg-state`, `tpg-test-pattern`

## tpg-test-pattern

**Description** Indicates a number that specifies the test pattern transmitted in the IMA control protocol (ICP) cell (octet 17) on the link during the inverse multiplexing over ATM (IMA) test pattern procedure.

**Usage** The valid range is from -1 to 255. The default is -1.

**Example** `set tpg-test-pattern = -1`

**Location** IMAGROUP

IMA-GROUP-STAT

IMA-GROUP-STAT:ima-rt

**See Also** `tpg-state`, `tpg-test-link`

## tpptest-status

**Description** Read-only. Indicates the current state of the test pattern procedure.

**Usage** This read-only parameter has the following possible values:

- disabled—Test pattern procedure is currently disabled on this link
- operating—Test pattern procedure is currently operating on this link
- link-fail—Test pattern procedure has failed on this link

**Example** tptest-status = disabled

**Location** IMA-GROUP-STAT

**See Also** tptest-state, tptest-link

## traceroute

**Description** *Not used.*

**Location** TERMINAL-SERVER:terminal-mode-configuration

## traffic-descr-index

**Description** *Not currently used.* Specifies an index to the atmTrafficDescrParamTable defined in RFC 1695. This traffic descriptor is used when establishing switched virtual channels for use as SVCC-based RCCs to or from PNNI logical group nodes.

**Location** ATM-QOS

## traffic-descriptor-index

**Description** Read-only. Indicates the traffic descriptor index.

**Usage** Read-only parameter with a numeric range of 0 to 4294967295.

**Example** traffic-descriptor-index = 1234

**Location** ATM-QOS

## traffic-descriptor-type

**Description** Specifies the Asynchronous Transfer Mode (ATM) traffic descriptor type as defined in RFC 2514, *Definitions of Textual Conventions and OBJECT-IDENTITIES for ATM Management*.

**Usage** Valid values are as follows:

- unknown-traffic-descr—Currently not used.
- noclp-noscr (the default)—With no cell loss priority (CLP) and no sustainable cell rate (SCR).
- noclp-scr—With no CLP, but with SCR.
- clp-notagging-scr—With CLP, no tagging, and with SCR.
- clp-tagging-scr—With CLP, tagging, and SCR.
- clp-transparent-noscr—With CLP transparent and no SCR.
- clp-transparent-scr—With CLP transparent and with SCR.
- noclp-tagging-noscr—With no CLP, tagging and no SCR.
- noclp-noscr-cdvt—With no CLP, no SCR, and with cell delay variation tolerance (CDVT) defined.
- noclp-scr-cdvt—With No CLP, with SCR and CDVT defined.
- clp-notagging-scr-cdvt—With CLP, with no tagging, with SCR and CDVT defined.
- clp-tagging-scr-cdvt—With CLP and tagging and with SCR and CDVT defined.
- clp-notagging-mcr—With CLP, with no tagging, and MCR defined.

**Dependencies** If you set traffic-descriptor-type to clp-tagging-scr, noclp-tagging-noscr, or clp-tagging-scr-cdvt, the SNMP tag-or-discard field is set to tag. Setting traffic-descriptor-type to all other traffic descriptor types sets the SNMP tag-or-discard field to discard (the default). Following are the allowable combinations of ATM service category and traffic descriptor type:

### ATM service categories

Variable bit rate (VBR)-real time  
Variable bit rate (VBR)-nonreal time

Constant bit rate (CBR)

Unspecified bit rate (UBR)

### Settings for traffic-descriptor-type

noclp-scr  
clp-notagging-scr  
clp-tagging-scr  
clp-transparent-scr  
noclp-scr-cdvt  
clp-notagging-scr-cdvt  
clp-tagging-scr-cdvt  
clp-notagging-mcr  
noclp-noscr  
clp-transparent-noscr  
noclp-noscr-cdvt  
noclp-noscr  
noclp-tagging-noscr  
noclp-noscr-cdvt

**Location** ATM-QOS

**See Also** tag-or-discard

## transit-delay

**Description** Specifies the estimated number of seconds it takes to transmit a link state update (LSU) packet over the interface. Before transmission, link state advertisements (LSAs) contained in the LSU packet have their ages incremented by the amount you specify.

**Usage** Specify a number greater than 0 (zero). The value you specify must take into account transmission and propagation delays. The default is 1.

**Example** set transit-delay = 5

IP-INTERFACE

CONNECTION:ip-options:ospf-options

## transit-number

**Description** *Not used.* Specifies an Interexchange Carrier (IEC) for long-distance ISDN Primary Rate Interface (PRI) calls.

**Location** CONNECTION:telco-options

## transmit-power

**Description** Read-only. Indicates the current transmission power the transceiver is using, reported in decibels under one milliwatt (dBm).

**Usage** The transmit-power value is read-only.

**Example** transmit-power = 10

**Location** HDLSL2-STAT:physical-statistic

SHDSL-STAT:physical-statistic

## transmit-sdu-size

**Description** Specifies the size of the transmit service data unit (SDU) in octets.

**Usage** Specify a value between 1 and 2000 octets. The default value is 1 (one).

**Example** set transmit-sdu-size = 128

**Location** CONNECTION:atm-aal-options

## transmitted-rs-blocks

**Description** Read-only. Indicates the number of transmitted Reed-Solomon blocks. Indicates the number of transmitted ADSL superframes (blocks) for Centillium-based line-interface modules (LIMs) and Stinger MRT units.

**Usage** The transmitted-rs-blocks value is read-only.

**Example** transmitted-rs-blocks = 416772

**Location** AL-DMT-STAT:physical-statistic

**See Also** received-rs-blocks  
incoming-cells

## transparentpvc

**Description** Read-only. Indicates whether a permanent virtual circuit (PVC) is point-to-point and transparent.

**Usage** Read-only parameter with the following possible values:

- yes—PVC is point to point and transparent.
- no—PVC is not point to point and transparent.

**Example** transparentpvc = yes

**Location** FRPVC-STAT

## trap-optimization-enabled

**Description** The trap-optimization-enabled parameter optimizes the number of traps generated for slot status change.

**Usage** Valid values are as follows:

- yes—The system optimizes the number of traps generated for slot status change.
- no (the default)—The system generates all traps.

**Example** set trap-optimization-enabled = yes

**Location** TRAP

## trap-sequencing

**Description** 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-enable* parameter must be set to *yes*).

**Usage** Valid values are as follows:

- *yes*—Enables sequencing.
- *no* (the default)—Disables sequencing.

**Example** `set trap-sequencing = yes`

**Location** TRAP

## trap-shelf-clli

**Description** Configures the system to send the CLLI information with traps.

**Usage** Valid values are as follows:

- *yes*—Sends the CLLI information with traps.
- *no*—Does not send the CLLI information with traps. This is the default.

**Example** `set trap-shelf-clli = yes`

**Location** TRAP

## tree-oid-mask

**Description** Specifies a mask in hexadecimal format for comparing subidentifiers in an object identifier (OID).

**Usage** Specify a mask in hexadecimal of up to 16 bytes. Comparison of subidentifiers can be omitted by specifying 0 (zero). The default is `ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff`.

**Example** `set tree-oid-mask =  
ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff`

**Location** VACM-VIEW-TREE

**See Also** `tree-type`

## tree-type

**Description** Specifies whether an object identifier (OID) is made accessible or not.

**Usage** Valid values are as follows:

- *included*—Specifies that the OID is accessible. This is the default.
- *excluded*—Specifies that the OID is not accessible.

**Example** `set tree-type = excluded`

**Location** `VACM-VIEW-TREE`

**See Also** `tree-oid-mask`  
`tree-view-properties`

## trellis-encoding

**Description** Enables or disables trellis encoding, which is a method of forward error correction.

The use of trellis encoding is specified in the discrete multitone (DMT) standard. Disabling it can increase performance, at the cost of becoming noncompliant with the standard.

**Usage** Valid values are as follows:

- `yes`—Enables trellis encoding. This is the default.
- `no`—Disables trellis encoding.

**Example** `set trellis-encoding = yes`

**Location** `AL-DMT:line-config`

## trunk-daughter-type

**Description** Read-only. Indicates the type of trunk daughter module present in a Stinger unit.

**Usage** Valid values for the read-only parameter are as follows:

- `trunk-daughter-none`
- `trunk-daughter-oc3-quad`
- `trunk-daughter-ds3`
- `trunk-daughter-oc3-ds3-combo`
- `trunk-daughter-oc3-single`
- `trunk-daughter-ds3-single`
- `trunk-daughter-e3`
- `trunk-daughter-e3-single`
- `trunk-daughter-2oc3-4ds3`
- `trunk-daughter-2stm1-4e3`
- `trunk-daughter-oc3-ver2`
- `trunk-daughter-ima-8t1`
- `trunk-daughter-ima-8e1`
- `trunk-daughter-16oc3`
- `trunk_daughter_types`



**Example** trunk-daughter-type = trunk-daughter-ds3

**Location** TRUNK-DAUGHTER-DEV

## trunk-group

**Description** *Not currently used.* Specifies a trunk-group number.

**Location** AL-DMT:line-config

CALL-ROUTE

DS3-ATM:line-config

E3-ATM:line-config

HDSL2:line-config

OC3-ATM:line-config

SDSL:line-config

SHDSL:line-config

## trunklinkindex

**Description** Read-only. Indicates the data link connection identifier (DLCI) member index for a trunk link.

**Usage** Read-only parameter with a range of 0 to 65535.

**Example** trunklinkindex = 8

**Location** FRPVC-STAT

## ts-idle-mode

**Description** *Not supported.* Specifies the number of seconds a terminal-server session can remain idle before being terminated.

**Location** ANSWER-DEFAULTS:session-info

CONNECTION:session-options

**See Also** session-info, session-options

## ts-idle-timer

**Description** *Not supported.* Specifies when to reset the terminal-server idle-session timer.

**Location** ANSWER-DEFAULTS:session-info

CONNECTION:session-options

**See Also** session-info, session-options

## ttone-lead

**Description** Specifies the measurement leads for the copper loop test (CLT) module trace tone test.

**Usage** Specify one of the following values:

- tip-ring—Uses tip and ring measurement leads. This is the default value.
- tip-sleeve—Uses tip and sleeve measurement leads.
- ring-sleeve—Uses ring and sleeve measurement leads.

**Example** `set ttone-lead = ring-sleeve`

**Location** CLT-COMMAND

## ttone-level

**Description** Specifies the trace tone send level for the copper loop test (CLT) module trace tone test.

**Usage** Specify the level in dBm in a range from -10dBm to 10dBm. The default value is 0.

**Example** `set ttone-level = 2`

**Location** CLT-COMMAND

## ttone-period

**Description** Specifies the trace tone period for the copper loop test (CLT) module trace tone test.

**Usage** Specify the period in minutes over a range of 1 to 120 minutes. The default is 60 minutes.

**Example** `set ttone-period = 30`

**Location** CLT-COMMAND

## tunnel-accounting

**Description** Enables or disables RFC 2867 RADIUS tunnel accounting.

**Usage** Specify one of the following values:

- no—Disables RFC2867 RADIUS tunnel accounting. This is the default.
- yes—Enables RFC2867 RADIUS tunnel accounting.

**Example** `set tunnel-accounting = yes`

**Location** EXTERNAL-AUTH:rad-acct-client

## tunneling-protocol

**Description** Specifies a protocol to establish a tunnel for this connection.

**Usage** Specify one of the following values:

- disabled—Does not use tunneling for this connection.
- l2tp-protocol— Uses Layer 2 Tunneling Protocol (L2TP).
- atmp-protocol (the default)— Uses Ascend Tunnel Management Protocol (ATMP).

**Example** set tunneling-protocol = l2tp-protocol

**Location** CONNECTION:tunnel-options

## tunnel-server-pre-sccrq-lookup

**Description** Enables or disables a lookup for a tunnel-server profile when a password is not available for a tunnel request.

**Usage** Specify yes or no. The default is no.

- yes—If the tunnel password is not available, the system looks for a matching tunnel-server profile before the Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) sends a Start Control Connection Request (SCCRQ) packet.
- no—The system looks for a matching tunnel-server profile after the system receives a L2TP Start-Control-Connection-Reply (SCCRP) packet from the L2TP network server (LNS).

**Example** set tunnel-server-pre-sccrq-lookup = yes

**Location** L2-TUNNEL-GLOBAL:l2tp-config

## tx-avail-cellrate

**Description** Read-only. Indicates the current cell rate (truncated value in cells per second) provided by this inverse multiplexing over ATM (IMA) group in the transmit direction, considering all the transmit links in the active state.

**Usage** The valid range for this read-only value is from 0 through 2147483647.

**Example** rx-avail-cellrate = 7188

**Location** IMA-GROUP-STAT

## tx-cell-payload-scramble-disabled

**Description** In transmitted cells, enables or disables scrambling of the 48-byte Asynchronous Transfer Mode (ATM) payload.

**Usage** Valid values are as follows:

- **yes**—Disables scrambling of the 48-byte ATM payload in transmitted cells.
- **no**—Enables scrambling of the 48-byte ATM payload in transmitted cells. This is the default.

**Example** `set tx-cell-payload-scramble-disabled = yes`

**Dependencies** Do not set `tx-cell-payload-scramble-disabled` to `yes` unless the receiving switch has disabled the corresponding descramble function.

**Location** `OC3-ATM:line-config`

**See Also** `rx-cell-payload-descramble-disabled`  
`tx-scramble-disabled`

## tx-k1-byte-value

**Description** Read-only. Indicates the current value of the K1 byte transmitted on the protection channel in an automatic protection switching (APS) system.

**Usage** The valid range for this read-only parameter is from 0 through 255.

**Example** `tx-k1-byte-value = 0`

**Location** `APS-STAT`

## tx-k2-byte-value

**Description** Read-only. Indicates the current value of the K2 byte transmitted on the protection channel in an automatic protection switching (APS) system.

**Usage** The valid range for this read-only parameter is from 0 through 255.

**Example** `tx-k2-byte-value = 0`

**Location** `APS-STAT`

## tx-lid

**Description** Specifies a number that identifies the transmit link. This parameter is read-only.

**Usage** The number can be from 0 through 31. The default is 0.

**Example** `tx-lid = 0`

**Location** `DS1-ATM-STAT:ima-link-status`

**See Also** `near-end-tx-link-state`, `rx-lid`, `valid-intervals`

## tx-min-num-links

**Description** Specifies the minimum number of active transmission (Tx) links required for an inverse multiplexing over ATM (IMA) group to remain in operational state.

**Usage** Specify a number from 1 to 8. The default is 1.

**Example** `set tx-min-num-links = 1`

**Location** IMAGROUP

## tx-num-active-links

**Description** Read-only. Indicates the number of links which are configured to transmit and are currently active in this inverse multiplexing over ATM (IMA) group.

**Usage** The valid range for this read-only value is from zero (0) to 24.

**Example** `tx-num-active-links = 2`

**Location** IMA-GROUP-STAT

## tx-num-config-links

**Description** Read-only. Indicates the number of links that are configured to transmit in this inverse multiplexing over ATM (IMA) group. This parameter overwrites the value of the `imaGroupNumRxActLinks` attribute when the IMA group is configured in the Symmetrical Configuration group symmetry mode.

**Usage** The valid range for this read-only parameter is from zero (0) to 24.

**Example** `tx-num-config-links = 2`

**Location** IMA-GROUP-STAT

## tx-oam-label-value

**Description** Read-only. Indicates the IMA operations and maintenance (OAM) label value transmitted by the near end (NE) inverse multiplexing over ATM (IMA) unit.

**Usage** Valid values for this read-only parameter are from one (1) to 255.

**Example** `tx-oam-label-value = 3`

**Location** IMA-GROUP-STAT

## tx-scramble-disabled

**Description** Enables or disables scrambling of the entire Asynchronous Transfer Mode (ATM) transmit stream.

**Usage** Valid values are as follows:

- **yes**—Specifies that scrambling of the entire ATM transmit stream is disabled.
- **no** (the default)—Specifies that scrambling of the entire ATM transmit stream is enabled.

**Example** `set tx-scramble-disabled = yes`

**Dependencies** Set `tx-scramble-disabled` to `yes` only if the receiving switch has disabled the corresponding descramble function.

**Location** `OC3-ATM:line-config`

## tx-sdu-size

**Description** The maximum ATM adaptation layer 5 (AAL5), common part convergence layer (CPCS), service data unit (SDU) size that is supported in the transmit direction of this virtual channel connection (VCC).

**Usage** Specify the number of octets in a range for 0 to 65535. The default value is 0.

**Example** `set tx-sdu-size = 32`

**Location** `ATM-VCL-CONFIG`

## tx-stuffs-counter

**Description** Read-only. Indicates the count of stuff events inserted in the transmit direction.

**Usage** The valid range for this read-only parameter is from 0 through 2147483647

**Example** `tx-stuffs-counter = 0`

**Location** `DS1-ATM-STAT:ima-link-statistic`

## tx-timing-ref-link

**Description** Read-only. Indicates the index of the transmit timing reference link to be used by the near-end for inverse multiplexing over ATM (IMA) data cell clock recovery from the Asynchronous Transfer Mode (ATM) layer.

**Usage** Valid values for this read-only parameter are from 0 through 24. The distinguished value of zero is used if no link has been configured in the IMA group, or if the transmit timing reference link has not yet been selected.

**Example** `tx-timing-ref-link = 1`

**Location** `IMA-GROUP-STAT`

## tx-traffic-desc

**Description** Specifies the ATM traffic descriptor index applied to the transmit direction of the virtual channel link (VCL).

**Usage** Specify a numeric value in the range 0 to 4294967295. The default value is 1.

**Example** `set tx-traffic-desc = 100`

**Location** ATM-VCL-CONFIG  
ATM-VPL-CONFIG

## type

**Description** Specifies or indicates, according to the profile, the following information:

- In the error profile, `type` indicates the type of error that has occurred.
- In `filter:input-filters` or `filter:output-filters` profiles specifies the type of filter. The type determines which filter specification is used. The system applies only the settings in the corresponding subprofile of the filter specification
- In the `pnmi-route-addr` profile, `type` specifies the type of Private Network-to-Network Interface (PNNI) connectivity from the advertising node to the address prefix.
- In the `pnmi-summary-addr:addr-index` profile, `type` specifies the type of summary being described.
- In the `snmpv3-notification` profile, `type` indicates the type of notification to be generated. *This field is for future use. The agent does not generate INFORM protocol data units (PDUs).*

**Usage** Valid values are as follows:

- For the error profile, this read only parameter has a range of 0 to 4294967295.
- For the `filter:input-filters` or `filter:output-filters` profiles specify one of the following filter types:
  - `generic-filter` (the default)—Generic filters can match any packet, regardless of its protocol type or header fields. The filter specifications operate together to define a location in a packet and a hexadecimal value to compare to it.
  - `ip-filter`—IP filters affect only IP and related packets. They make use of high-level information in packets (for example, protocol numbers, logical addresses, and TCP or UDP ports).
  - `route-filter`—Route filters are applied to RIP update packets to exclude routes from the local system's routing table, or to include routes in the table only after modifying their metrics.
  - `tos-filter`—Type of service (TOS) filters are used to enable proxy-quality-of-service (QoS) handling for packets that match the filter specification. For TOS filters, the forwarding action in the filter has no effect.

- For `pnni-route-addr` profile, specify one of the following PNNI connectivity type values:
  - `other`
  - `internal`—Directly attached to the logical node advertising the address.
  - `exterior`—Reachable through the PNNI routing domain, but not located in the PNNI routing domain. This is the default.
  - `reject`—If the address prefix is matched, the unit discards the message as unreachable. This type of connectivity is used by some protocols to aggregate routes.
- For the `pnni-summary-addr:addr-index` profile, specify one of the following values:
  - `internal-summary` (the default).
  - `external-summary`
- For the `snmpv3-notification` profile this read-only parameter has the following values:
  - `trap`—Unconfirmed notification
  - `inform`—Confirmed notification

**Example** `set type = exterior`

**Location** `ERROR`

`FILTER:input-filters[n]`

`FILTER:output-filters[n]`

`PNNI-ROUTE-ADDR`

`PNNI-SUMMARY-ADDR:Addr-Index`

`SNMPV3-NOTIFICATION`

## type-of-service

**Description** Specifies the type of service of the data stream. In the type of service (TOS) byte of a packet, the 4 bits following the priority bits (specified in the precedence setting) are used to choose a link according to the type of service.

**Usage** According to the profile, as follows:

- When TOS is enabled in a `connection` profile, you can set the type of service to one of the following values for the WAN connection.
- In a filter profile, specifying a `type-of-service` value causes the system to use that value for packets that match the filter.

When TOS is enabled, specify one of the following values:

- `normal` (the default)—Establish normal service.
- `cost`—Minimize monetary cost.
- `reliability`—Maximize reliability.
- `throughput`—Maximize throughput.
- `latency`—Minimize delay.

**Example** `set type-of-service = cost`



**Dependencies** For this setting to apply, TOS and IP routing must be enabled in the connection profile, or TOS must be specified as the filter type in the filter profile.

**Location** CONNECTION:ip-options:tos-options

FILTER:input-filters:tos-filter

FILTER:output-filters:tos-filter

**See Also** tos-filter

tos-options

## U

### ubr

**Description** Enables or disables unspecified bit rate (UBR) traffic in this queue.

**Usage** Valid values are as follows:

- yes—Specifies that the queue supports ATM unspecified-bit-rate (UBR) traffic.
- no—Specifies that the queue does not support UBR traffic. This is the default.

For each queue, one or more ATM services categories can be set to yes. The ubr parameter must be set to yes for at least one and no more than two of the active queues assigned to a line interface module (LIM), control module, or trunk.

**Example** set ubr = yes

**Location** SWITCH-CONFIG:atm-parameters:outgoing-queue

**See Also** cbr

real-time-vbr

### udp-cksum

**Description** Enables or disables UDP checksums. You might want to enable checksums if data integrity is of the highest concern for your environment, and having redundant checks is important. This setting is also appropriate if your UDP-based servers are located on the remote side of a WAN link that is prone to errors.

**Usage** Specify yes or no. The default is yes.

- yes—Enables UDP checksums. With this setting, the Stinger unit generates a checksum whenever it sends out a UDP packet.
- no—Disables checksums.

**Example** set udp-cksum = yes

**Location** IP-GLOBAL

## udp-port

**Description** Specifies a UDP port number to use for a tunnel. Both ends of the tunnel must agree on the number.

- In an Ascend Tunnel Management Protocol (ATMP) Home Agent configuration, the setting identifies the port Foreign Agents must use to establish tunnels with the Home Agent.
- In an ATMP mobile-client profile, the setting specifies the UDP port expected by one or both of the ATMP Home Agents. If the mobile-client profile specifies a Home Agent IP address that includes a port number, the value overrides this parameter.

**Usage** Specify a UDP port number. The default is 5150.

**Example** `set udp-port = 5100`

**Dependencies** If you change the `udp-port` setting, the new value does not take effect until you reset the system.

**Location** ATMP  
CONNECTION:tunnel-options

## unavailable-second

**Description** Read-only. Indicates the number of 1-second intervals for which the HDSL2 line is unavailable. The HDSL2 line becomes unavailable at the onset of 10 contiguous severely errored seconds (SESSs). Once unavailable, the HDSL2 line becomes available at the onset of 10 contiguous seconds with no SESSs.

**Usage** The valid range for this read-only value is from 0 to 4294967295.

**Example** `unavailable-second = 0`

**Location** HDLSL2-STAT:physical-statistic  
SHDSL-STAT:physical-statistic

## unavailable-secs

**Description** Read-only. Indicates the count of 1-second intervals, within the current 15-minute interval, during which the inverse multiplexing over ATM (IMA) group traffic state machine is unavailable.

**Usage** The valid range for this read-only parameter is from zero (0) to 2147483647.

**Example** `unavailable-secs = 56`

**Location** IMA-GROUP-STAT:ima-group-statistic

## uncorrected-hec-error-count

**Description** Read-only. Number of uncorrected header check sequence (HCS) errors since the Stinger unit was last reset.

**Usage** The uncorrected-hec-error-count value is read-only.

**Example** uncorrected-hec-error-count = 0

**Location** DS3-ATM-STAT  
E3-ATM-STAT  
OC3-ATM-STAT

## unit-type

**Description** Indicates or specifies, according to the profile, the operating mode of a symmetric digital subscriber line (SDSL) module.

**Usage** Valid values are as follows:

- In the al-dmt-stat and sdsl-stat profile, the unit-type parameter is read-only. It can have one of the following values:
  - coe—Central office equipment.
  - cpe—Customer premises equipment.
- In an sdsl profile, you must set the unit-type parameter to coe.

**Example** set unit-type = cpe

**Location** AL-DMT-STAT:physical-status  
SDSL:line-config  
SDSL-STAT:physical-status  
SHDSL:line-config

## unknown-cards

**Description** Specifies the action to take when the code image for newly supported modules is present in a tar file.

**Usage** Valid values are as follows:

- auto—Loads the code image if a module of that type is installed. Otherwise, The image is not loaded. This is the default.
- load—Loads the code image when one is present in the tar file.
- skip—Does not load the code image when one is present in the tar file.

**Example** `set unknown cards = auto`

**Dependencies** A module is considered present in the system if a Slot-Type profile exists for that module type. The system creates a Slot-Type profile when it first detects the presence of a module, and does not delete the profile unless the administrator uses the Slot `-r` command to permanently remove a module that is no longer installed in the system, or clears 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.

**Location** `LOAD-SELECT`

## `update-threshold`

**Description** Specifies the update threshold on the Simple Network Time Protocol (SNTP) server, in seconds.

**Usage** Specify the number of seconds from zero (0) to 2147483647.

**Example** `set update-threshold = 10`

**Dependencies** This field is applied only if the `enabled` parameter in the `sntp-info` subprofile is set to `passive`.

**Location** `IP-GLOBAL:sntp-info`

## `update-time`

**Description** Read-only. Indicates the absolute time at which this context was last updated.

**Usage** Read-only parameter with a numeric range of 0 to 4294967295.

**Example** `update-time = 123`

**Location** `REDUNDANCY-STATS:context-stats`

## `up-down-threshold`

**Description** Specifies the number of times during the specified error-averaging period that a line is enabled and disabled by a modem before the modem is considered nonfunctional.

**Usage** The default value is 3 counts.

**Example** `up-down-threshold = 3`

**Location** `LIM-SPARING-CONFIG:auto-lim-sparing-config:lim-sparing-config[n]`

## up-dwn-cntr

**Description** Read-only. Indicates the number of times the interface transitions from a DOWN state to an UP state.

**Usage** Read-only parameter with a value ranging from 0 to 4294967295.

**Example** up-dwn-cntr = 4

**Location** AL-DMT-STAT:physical-statistic  
SDSL-STAT:physical-statistic  
HDSL2-STAT:physical-statistic  
IDSL-STAT:physical-statistic  
SHDSL-STAT:physical-statistic

## up-status

**Description** Read-only. Indicates the status of a device.

**Usage** The up-status parameter is read-only. Valid values are as follows:

- idle-up-status—Indicates that the device is not currently in use.
- reserved-up-status—Indicates that the device is not currently in use and should not be used until all idle devices of the same type are in use.
- assigned-up-status—Indicates that the device is in use.

**Example** up-status = idle-up-status

**Location** DEVICE-STATE

**See Also** device-address  
device-state  
reqd-state

## upstream-end-bin

**Description** Specifies the ending frequency bin for upstream transmission.

**Usage** The valid range is 0 to 31 for 12- and 24-port line interface modules (LIMs) and 6 to 31 for 48-port LIMs. The default value is 31.

**Example** set upstream-end-bin = 31

**Location** AL-DMT

## up-stream-latency

**Description** Read-only. Indicates the operational upstream latency.

**Usage** The up-stream-latency parameter is read-only. Valid values are as follows:

- none— Indicates that the line is not operational.
- fast— Indicates that the setting for the least up stream latency is in effect.
- interleave— Indicates that the interleave latency (greater than fast) is in effect.

**Example** up-stream-latency = fast

**Location** AL-DMT-STAT:physical-status

**See Also** down-stream-latency

## up-stream-rate

**Description** Read-only. Indicates the upstream data rate for the symmetric digital subscriber line (SDSL) interface in bits per second.

**Usage** the up-stream-rate parameter is read-only. A value of 0 (zero) indicates that the data rate is unknown.

**Example** up-stream-rate = 0

**Dependencies** SDSL interfaces ensure maximum throughput for the particular condition of the line. The better the line quality, the higher the data rate.

**Location** SDSL-STAT:physical-status

## up-stream-rate-fast

**Description** Read-only. Indicates the upstream data rate in bits per second when up stream latency has a value of fast.

**Usage** A value of 0 (zero) means that latency is set to interleave or the data rate is unknown.

**Example** up-stream-rate-fast = 0

**Location** AL-DMT-STAT:physical-status

**See Also** down-stream-rate-interleave  
down-stream-latency  
up-stream-latency  
up-stream-rate-interleave

## up-stream-rate-interleave

**Description** Read-only. Indicates the upstream data rate in bits per second when up-stream-latency has a value of interleave.

**Usage** A value of zero means that latency is set to fast or the data rate is unknown.

**Example** up-stream-rate-interleave = 0

**Location** AL-DMT-STAT:physical-status

## upstream-start-bin

**Description** Specifies the starting frequency bin for upstream transmission.

**Usage** The valid range is 0 to 31 for 12-port and 24-port line interface modules (LIMs), and 6 to 31 for 48-port LIMs. The default value is 6.

**Example** `set upstream-start-bin = 31`

**Location** AL-DMT

**See Also** downstream-end-bin, downstream-start-bin, gmt-offset, sntp command

## use-answer-for-all-defaults

**Usage** Specifies whether values in the Answer-Defaults profile override values in the default Internet profile when the Stinger unit uses RADIUS to validate an incoming call.

**Usage** Valid values are as follows:

- **yes** (the default)—Specifies that the Stinger unit uses the Answer-Defaults profile for defaults. When you specify **yes**, the Stinger unit falls back to the values specified in the Answer-Defaults profile for options that are not specified in a given external authentication profile.
- **no**—Specifies that the Stinger unit uses the default Internet profile for defaults. When you specify **no**, the Stinger unit uses defaults for options not specified in a given external authentication profile.

**Example** `set use-answer-for-all-defaults = no`

**Location** ANSWER-DEFAULTS

**See Also** profiles-required

## used-count

**Description** Read-only. Indicates the number of times this device was used.

**Usage** Read-only numeric parameter with a range of 0 to 4294967295.

**Example** `used-count = 10`

**Location** DEVICE-STATE

## use-exceeded-enabled

**Description** Specifies whether the system generates a trap (notification) when either a specific port has exceeded the number of DS0 minutes allocated to it or the system DS0 usage has been exceeded.

**Usage** Valid values are as follows:

- **yes** (the default)—Specifies that the system generates a trap when a specific port has exceeded the number of DS0 minutes allocated to it, or the system DS0 usage has been exceeded.
- **no**—Specifies that the system does not generate a trap when a specific port has exceeded the number of DS0 minutes allocated to it, or the system DS0 usage has been exceeded.

**Example** `set use-exceeded-enabled = no`

**Location** TRAP

**See Also** port-enabled

## use-group-permissions

**Description** Enable/disable the user's access to all the allow-xxx settings in the user-group profile specified by the user-group parameter.

**Usage** Valid values are as follows:

- **yes**—Specifies that the user has access to all commands permitted by the allow-xxx setting in the user-group profile, and that the allow-xxx settings in the user profile are ignored.
- **no** (the default)—Specifies that the user does not have access to the commands permitted by the allow-xxx settings in the user-group profile, and that only the commands permitted by the allow-xxx settings in the user profile apply.

**Example** `set use-group-permissions = yes`

**Location** USER-GROUP

## user

**Description** The user profile associated with the user who entered the command indicated in the cmd-log profile information parameter.

**Usage** This parameter is read-only.

**Example** `user = admin`

**Location** cmd-log



## user-acct-expiration-date

**Description** Expiration date for this user account. Complex field.

**Usage** The following sample commands specify the expiration date for the user account remote:

```
admin> read user remote
USER/test read
admin> list user-acct-expiration-date
[in USER/remote:user-acct-expiration-date]
weekday = Monday
month = January
year = 1990
day = 1
admin> set month = December
admin> set year =2005
admin> set day = 31
admin> write -f
USER/remote written
```



**Note** The parameter weekday is not configurable.

**Example** user-acct-expiration-date = { Saturday November 2006 11 }

**Location** USER

## user-group

**Description** 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.

**Usage** Specify the name of a valid user-group profile.

**Example** set user-group = mygroupname

**Location** USER

## user-passwd-expiration-date

**Description** User password expiration date. Complex field.

**Usage** The following sample commands specify the expiration date for the password of the user account remote:

```
admin> read user remote
USER/test read
admin> list user-passwd-expiration-date
[in USER/remote:user-passwd-expiration-date]
weekday = Monday
month = January
year = 1990
day = 1
admin> set month = dec
admin> set year = 2003
admin> set day = 31
admin> write -f
USER/remote written
```



**Note** The parameter weekday is not configurable.

**Example** user-passwd-expiration-date = { Sunday January 2004 11 }

**Location** USER

## user-profile

**Description** Specifies or indicates, according to the profile, a user profile name as follows:

- In the ip-global profile, user-profile specifies the name of the default user profile associated with Telnet sessions.
- In a serial profile, user-profile specifies the name of the default user profile associated with serial access to the Stinger command-line interface.
- In an error profile, user-profile indicates the name of the user that reset the unit.

**Usage** Valid values are as follows:

- In the ip-global or serial profile, specify the name of a user profile. Defaults are as follows. In either profile, a null value specifies that the user must log in explicitly.
  - For the ip-global profile, the default is null.
  - For the serial profile, the default is admin.
- In an error profile, the user-profile parameter is read-only.

**Example** set user-profile = default

**Location** ERROR  
IP-GLOBAL  
SERIAL

## user-second-level-authentication

**Description** Enables/disables two-level user authentication for the different types of administrative access to a Stinger system.

**Usage** Specify one of the following the values:

- none (the default)—Second level authentication is disabled for the system.
- console-only—Second level authentication is enabled only for console access.
- telnet-only—Second level authentication is enabled only for console access.
- modem-only—Second level authentication is enabled only for modem access.
- control-bus-only: Second level authentication is required only for control-bus access (from a remote shelf to a host Stinger system).
- console-modem-only—Second level authentication is enabled for console and modem access.
- console-telnet-only—Second level authentication is enabled for console and telnet access.
- telnet-modem-only—Second level authentication is enabled only for telnet and modem access.
- console-control-bus-only—Second level authentication is required for console and control-bus access.
- telnet-control-bus-only—Second level authentication is required for telnet and control-bus access.
- modem-control-bus-only—Second level authentication is required for telnet and control-bus access.
- console-telnet-modem-only—Second level authentication is enabled for console, telnet, and modem access.
- console-telnet-ctrl-bus-only—Second level authentication is enabled for console, telnet and control-bus access.
- console-modem-ctrl-bus-only—Second level authentication is enabled for console, modem and control-bus access.
- modem-telnet-ctrl-bus-only—Second level authentication is enabled for modem, telnet, and control-bus access.
- system-level—Second level authentication is enabled system access.

**Example** set user-second-level-authentication = telnet-only

**Location** SYSTEM

## userstat-format

**Description** Customizes the output of the userstat command.

**Usage** Specify a series of conversion strings. You can enter up to 72 characters. The maximum width of the output string depends on the width of the fields present in the session listing output. If you enter a character without a percent sign (%), it is printed as a literal character in the session-listing output. You can enter one or more of the following strings:

| String | Field width | Output text | Meaning                                                   |
|--------|-------------|-------------|-----------------------------------------------------------|
| %i     | 10          | SessionID   | Unique ID assigned to the session                         |
| %l     | 10          | Line/Chan   | Physical address ( <i>shelf.slot.line/chan</i> )          |
| %s     | 11          | Slot:Item   | <i>Shelf:slot:item/logical-item</i> of the host port      |
| %r     | 11          | Tx/Rx Rate  | Transmit and receive rates                                |
| %d     | 3           | Svc         | A three-letter code showing the type of service           |
| %a     | 15          | Address     | IP address                                                |
| %u     | 14          | Username    | Connection profile name                                   |
| %c     | 10          | ConnTime    | Amount of time connected, in <i>hours:minutes:seconds</i> |
| %t     | 10          | IdleTime    | Amount of time idle, in <i>hours:minutes:seconds</i>      |
| %n     | 24          | Dialed#     | Number dialed if known                                    |

The default value of userstat-format causes the standard session-listing output format for the userstat command.

**Example** An administrator customizes the session-listing output to include only the Username, Svc, and ConnTime information, and enters an *at* sign (@) between the service and connection time for each session:

```
admin> read system
SYSTEM read

admin> set userstat-format = %u (%d) @ %c

admin> write
SYSTEM written

admin> userstat

Username Svc ConnTime
joeb (TCP) @ 1:22:34
jimmyq (TCP) @ 3:44:19
sallyg (TCP) @ 5:12:56

<end user list> 3 active user(s)
```

**Location** SYSTEM

**See Also** userstat command

## use-scroll-regions

**Description** Specifies whether the VT100 scroll-region commands are used to reduce screen redraws when the status screen is displayed.

**Usage** Valid values are as follows:

- **yes**—Specifies that the VT100 scroll-region commands are used to reduce screen redraws. This is the default.
- **no**—Specifies that the VT100 scroll-region commands is disabled. If the status screen is not redrawing properly, try setting Use-Scroll-Regions to no. This is the default.

**Example** `set use-scroll-regions = yes`

**Location** USER

**See Also** bottom-status, default-status

## use-short-address

**Description** Enables or disables use of a shorter address format for system-generated ATM addresses.

**Usage** Valid values are as follows:

- **no** (the default)—Uses 20-byte addresses.
- **yes**—Uses addresses of fewer than 20 bytes.

**Example** `set use-short-address = yes`

**Location** ATM-PREFIX

## use-trunk-groups

**Description** *Not used.*

**Location** SYSTEM

## use-vp-switching-workaround

**Description** Enables or disables virtual path (VP)-switching from the line interface module (LIM) in this slot to a trunk.

**Usage** Valid values are as follows:

- **yes**—LIM-to-trunk virtual path connections are configured for connections originating from this slot.
- **no** (the default)—LIM-to-trunk virtual path connections are not configured for connections originating from this slot.

**Example** set use-vp-switching-workaround = no

**Location** SLOT-STATIC-CONFIG/{ any-shelf any-slot N }

**See Also** need-max-vpswitching-vpis

## ustat-rsp-to-poll

**Description** Enables or disables sending of a USTAT message in response to a poll indicating an out-of-sequence protocol data unit (PDU).

**Usage** Select one of the following values:

- yes—Enables USTAT message for an out-of-sequence PDU.
- no—Disables USTAT message for an out-of-sequence PDU. This is the default.

**Location** ATM-IF-SIG-PARAMS [n] :gsaal-options

## utopia-address

**Description** *For internal use only.*

**Location** DS1-ATM-STAT

---

## V

### v42/mmp

**Description** *Not used.*

### validation-enable

**Description** Enables/disables validation, for Compact Remote shelves only. For the system to perform the ID comparison, validation must be enabled and `validation-id` must have a nonzero value.

**Usage** In the system profile, valid values are as follows:

- `yes`—Enables validation.
- `no` (the default)—Disables validation.

**Usage** In the `remote-shelf-config` profile, valid values are as follows:

- `system-defined`—Use the setting in the system profile to determine if validation is enabled for this shelf.
- `yes`—Enables validation.
- `no` (the default)—Disables validation.

**Example** `set validation-enable = system-defined`

**Dependencies** For the system to actually perform the ID comparison, validation must be enabled and `validation-id` in the `remote-shelf-config` profile must have a nonzero value.

**Location** `SYSTEM`

`REMOTE-SHELF-CONFIG:validation-config`

### validation-id

**Description** A validation ID to compare against the DIP-switch setting of the Compact Remote shelf. With a zero value, the system does not perform validation. With a nonzero value, the system compares the value to the binary DIP-switch setting of the remote shelf. If the values do not match exactly, RLIM service in the remote shelf is disabled.

**Usage** Specify an integer from 0 to 255.

**Example** `set validation-id = 255`

**Dependencies** If you specify a nonzero value, it must be unique within the hosted system. If you specify an ID that is already specified for another shelf, the system refuses to write the profile.

**Location** `REMOTE-SHELF-STAT:validation-status`

`REMOTE-SHELF-CONFIG:validation-config`

## validation-id-setting

**Description** The physical validation ID set by DIP switches on the remote shelf. This value is read from the remote shelf.

**Usage** This parameter is read-only. A valid value is an integer from 0 to 255.

**Location** REMOTE-SHELF-STAT:validation-status

## valid-cell-counter

**Description** Read-only. Indicates the total number of valid cells received by the unit.

**Usage** The Valid-Cell-Counter value is read-only.

**Example** valid-cell-counter = 0

**Location** OC3-ATM-STAT

**See Also** idle-cell-counter

## valid-entry

**Description** Enables or disables the filter specification. The system does not use a disabled filter specification when filtering a data stream.

**Usage** Specify yes or no. The default is no.

- yes—Enables the filter specification.
- no (the default)—Disables the specification.

**Example** set valid-entry = yes

**Location** FILTER:input-filters[n]  
FILTER:output-filters[n]  
TACL:permit-list[n]

## valid-intervals

**Description** Read-only. Indicates the number of previous 15-minute intervals for which valid data was collected.

**Usage** The valid range for this read-only parameter is from 0 through 96. The value is 96 unless the inverse multiplexing over ATM (IMA) link was added to the IMA group within the last 24 hours, in which case the value is the number of complete 15-minute intervals since the link was added to an IMA group.

**Example** valid-intervals = 96

**Location** DS1-ATM-STAT:ima-link-status  
IMA-GROUP-STAT



## value

**Description** Specifies a hexadecimal number to be compared to the packet data identified by the offset, len, and mask calculations.

**Usage** Specify a hexadecimal number, up to 12 bytes long. After you have entered the number, the system enters a colon (:) at the byte boundaries.

**Example** `set value = aaaa0300000080f3`

**Dependencies** This setting applies only if the type parameter in the input-filter or output-filter subprofile is set to generic-filter.

**Location** `FILTER:input-filters[n]:gen-filter`  
`FILTER:output-filters[n]:gen-filter`

## vcc-ident

**Description** Read-only. Indicates a unique virtual channel connection (VCC) identifier, made up of the interface address (shelf, slot, and modem numbers), the virtual path identifier (VPI), and the virtual channel identifier (VCI).

**Usage** Read-only value.

**Example** `vcc-ident* = { shelf-1 slot-10 47 0 35 }`

**Location** `ATMVCC-STAT`

## vcc-type

**Description** Read-only. Indicates the type of circuit.

**Usage** Read-only value with the following possible values:

- `connecting`—Point-to-point connecting. Always valid for an ATM circuit.
- `terminating`—Circuit is terminated.

**Example** `vcc-type = connecting`

**Location** `ATMVCC-STAT`

## vcc-vci n

**Description** Read-only. Indicates an array of 16 virtual channel identifiers (VCIs) for virtual circuit connections (VCCs) in Asynchronous Transfer Mode (ATM).

**Usage** This is a read-only parameter.

**Example** `vcc-vci[1] = greenham`

**Location** `OC3-ATM-STAT`

## vc-fault-management

**Description** *Not currently used.* Specifies the virtual circuit fault management type.

**Usage** Valid values are as follows:

- `none` (the default)—No fault management is performed on the virtual circuit.
- `segment loopback`—The system sends an operations, administration, and maintenance (OAM) F5 segment loopback cell to the remote device every 5 seconds.
- `end-to-end-loopback`—The system sends an OAM F5 end-to-end loopback cell to the remote device every 5 seconds.

**Example** `set vc-fault-management = none`

**Location** `CONNECTION station:atm-connect-options`

**See Also** `oam-support`  
`spvc-retry-limit`  
`vc-max-loopback-cell-loss`

## vci

**Description** Specifies or indicates, according to the profile, the virtual channel identifier (VCI) for an Asynchronous Transfer Mode (ATM) link, as follows.

- In the `atm-options` subprofile, `vci` specifies the first side of the circuit.
- In the `atm-connect-options` subprofile, `vci` specifies the second side of the circuit.
- In the `atmpvc-stat` and `atmvcc-stat` profiles, the `vci` value is read-only.

**Usage**

- In an `atm-options` or `atm-connect-options` subprofile, specify a number from 1 to 32767.
- In the `atmpvc-stat` and `atmvcc-stat` profiles, the `vci` value is read-only.

**Location** `CONNECTION:atm-options`  
`CONNECTION:atm-connect-option`  
`ATMPVC-STAT:vcc-members [n]`  
`ATMPVC-STAT:vcc-members:vcc-members`  
`ATMVCC-STAT:vcc-ident`

**See Also** `vpi`

## vc-max-loopback-cell-loss

**Description** *Not currently used.* Specifies the number of consecutive loopback cells that can be lost before the system clears the connection. When a permanent virtual circuit (PVC) is cleared, the interface is in an inactive state until the system can reestablish the connection.

**Usage** The default is 1.

**Example** `set vc-max-loopback-cell-loss = 1`

**Location** CONNECTION:atm-connect-options

**See Also** oam-support  
spvc-retry-limit  
vcc-vci

## vc-oam4-support n

**Description** Enables/disables specific F4 segment and end-to-end OAM processing on a Stinger VC-switching VPI. *N* is the index value.

**Usage** Valid values are as follows:

- yes (the default)—F4 segment and end-to-end processing for the specified VC-switching VPI is enabled.
- no—F4 segment and end-to-end processing for the specified VC-switching VPI is disabled.

## vc-switching-vpi [n]

**Description** An array listing up to 96 virtual path identifiers (VPIs), in addition to VPI 0, that the system uses for virtual channel (VC) switching.

**Usage** You can specify a VPI for each field in the array. The default is 0 (zero).

**Example** `set vc-switching-vpi 1 = 50`

**Dependencies** Consider the following:

- All VC-switching VPIs have a valid range specified by `vpi-vci-range`. All other VPIs are used for virtual path (VP) switching.
- Adding a VPI to a list of VC-switching VPIs causes the system to allocate more virtual channel connections (VCCs) for this port. You must make sure that the number of VCCs for other ports has been reduced to accommodate the increase in VCCs, because the system can support VCCs up to a limit of 48K on all trunk ports combined.
- Any change you make to a list of VPIs is effective immediately. To make the change, the system drops and reestablishes all connections.
- For a TRAM port, up to 96 VPIs can be specified. For a standard trunk port, only 64 VPIs can be configured.

- The Stinger controller's ATM application-specific integrated circuit (ASIC) supports up to 49,152 virtual connections across all trunk interfaces. If you specify additional VPI numbers to be used for VCCs, you must decrease the valid range of VCIs that can be assigned in combination with those VPIs.

This requirement allows you to allocate VCCs efficiently across trunk interfaces while remaining within the limits of ASIC capacity.

- If a connection uses a VPI, the system does not allow you to delete that VPI while the connection is active. To delete a VPI that is assigned to active connections, you must put those connections out of service administratively by setting `active` to `no` in the connection profiles.

**Location** DS3-ATM:line-config

E3-ATM:line-config

OC3-ATM:line-config

vds1

**Description** *Not supported.*

**Location** LOAD-SELECT

## vendor-option-string

**Description** Used to identify the system to the BRAS, AAA, or PPPoE server.

**Usage** Specify a text string of up to 31 characters.

**Example** `set vendor-option-string = stinger-001`

**Dependencies** This setting and the `if-ip` setting are mutually exclusive. This setting is currently not supported in the `dhcp-snooping` subprofiles.

**Location** `BRIDGE-GROUP:dhcp-snooping:circuit-id`  
`BRIDGE-GROUP:dhcp-snooping:remote-id`  
`BRIDGE-GROUP:pppoe-snooping:circuit-id`  
`BRIDGE-GROUP:pppoe-snooping:remote-id`

## verify-remote-host-name

**Description** Enables or disables verification of the hostname returned by the Layer 2 Tunneling Protocol (L2TP) network server (LNS).

When enabled, the L2TP access concentrator (LAC) compares the hostname returned by the LNS in the Start-Control-Connection-Reply (SCCRP) packet to the `server-auth-id` value configured in the local `tunnel-server` profile or the `Tunnel-Server-Auth-ID` attribute in a RADIUS profile. If the values do not match, the LAC terminates the tunnel request.

**Usage** Specify `yes` or `no`. The default is `no`.

- `yes`—Enables verification of the hostname returned by the LNS.
- `no`—Does not perform hostname verification.

**Example** `set verify-remote-host-name = yes`

**Location** `L2-TUNNEL-GLOBAL:l2tp-config`

## version

**Description** Indicates or specifies, according to the profile, one of the following:

- In the `error` profile, indicates the software version running when an error occurred.
- In the `imagroup` profile, specifies the inverse multiplexing over ATM (IMA) specification version.
- In the `circuit-id` profile, specifies the Relay agent version ID.

**Usage** Valid values are as follows:

- In the error profile, an alphanumeric read-only parameter with up to 24 characters.
- In the imagroup profile, specify one of the following values:
  - v1-0—ATM Forum IMA version 1.0
  - v1-1—ATM Forum IMA version 1.1 This is the default value.
- In the circuit-id profile, change this from the default 1 to a value of 257 or higher to interoperate with DHCP servers that zero-delimit suboption fields. The default value is 1.

**Example** `set version = v1-0`

**Location** ERROR

IMAGROUP

IP-GLOBAL:bootp-relay:relay-agent-information:circuit-id

BRIDGE-GROUP:dhcp-snooping:circuit-id

BRIDGE-GROUP:dhcp-snooping:remote-id

BRIDGE-GROUP:pppoe-snooping:circuit-id

BRIDGE-GROUP:pppoe-snooping:remote-id

## view-name

**Description** Specifies the name of a view in a view-based access control model (VACM) that acts as the link between a vacm-view-tree profile and a vacm-access profile.

**Usage** Specify a string of up to 32 characters.

**Example** `set view-name = view1`

**Location** VACM-VIEW-TREE:tree-properties

## view-tree-oid

**Description** Specifies the MIB object ID (OID) that represents the subtree for allowing or disallowing access in a view-based access control model (VACM).

**Usage** Specify up to 255 characters in dotted decimal format. The default is null.

**Example** `set view-tree-oid = 10.10.10.10`

**Location** VACM-VIEW-TREE:tree-properties

## vj-header-prediction

**Description** Enables or disables Van Jacobson prediction for TCP packets on session requests using encapsulation protocols that support Van Jacobson (VJ) compression.

**Usage** Valid values are as follows:

- yes (the default)—Enables VJ compression for TCP packets.
- no —Disables VJ compression for TCP packets.

**Example** `set vj-header-prediction = no`

**Location** ANSWER-DEFAULTS:ip-answer  
CONNECTION:ip-options

**See Also** ip-answer  
ip-options

## vlan-enabled

**Description** Enables or disables IEEE 802.1Q VLAN tagging on the virtual IP interface.

**Usage** Specify yes or no. The default is no.

**Example** `set vlan-enabled = yes`

**Location** IP-INTERFACE

## vlan-id

**Description** Specifies the VLAN ID for the virtual interface or profile. The `vlan-id` value is the IEEE 802.1Q VLAN tag value added to the IP packets associated with the IP data stream.

**Usage** In the `ip-interface`, `layer2-classifier`, and `service-options` profiles, you can specify a number from 0 through 4095. To maintain full compatibility with IEEE 802.1Q, Lucent recommends that `vlan-id` values of 0, 1 and 4095 not be assigned.

In the `vlan-ethernet` profile, the `vlan-id` value is read-only. It is set when you specify the VID profile identifier in the interface address, `{{shelf, slot, port }VID}` when creating a specific `vlan-ethernet` profile.

**Example** `set vlan-id = 42`

**Location** FLOW-SERVICES:flow-list [n]:layer2-classifier  
FLOW-SERVICES:flow-list [n]:service-options  
IP-INTERFACE  
VLAN-ETHERNET

## vlan-stack-tag-type

**Description** Two-byte hexadecimal value to be inserted in the EtherType field for stacked-VLAN frames. All stacked VLAN frames being transmitted/received on the Ethernet port will use this value in their EtherType field.

**Usage** The default value is 0x9100. For the sake of interoperability, this value is configurable. If the layer-2 core network is using a specific EtherType value for stacked VLAN frames, you must set the `vlan-stack-tag-type` parameter to that value. The default settings, for VLAN stacking of untagged frames is 91:00.

**Location** ETHERNET

## vlan-stack-user-vlan-id

**Description** Subscriber's 802.1Q VLAN ID to be used in stacked-VLAN frames for incoming traffic that contains untagged Ethernet frames.

**Usage** Valid values are from 0 to 4095. The value must be unique within the NSP VLAN. With the default zero value, VLAN stacking is disabled for the connection. When set to a nonzero value, VLAN stacking is enabled and the specified value is added to the frames as a VLAN tag that represents the user's connection within the context of an NSP. The default settings, for VLAN stacking of untagged frames is 0.

**Example** `set vlan-stack-user-vlan-id = 471`

**Dependencies** This parameter is applicable only in connection profiles. Although it also appears in both ethernet and vlan-ethernet profiles, the field is not applicable to those contexts.

**Location** CONNECTION:bridging-options  
ETHERNET  
VLAN-ETHERNET

## voice-detection

**Description** Read-only. A numeric value indicating the result of a copper loop test (CLT).

**Usage** This read-only parameter has the following possible values:

- 1—Voice signal not detected.
- 2—Voice signal detected.
- 3—Steady state indicates possible data traffic.
- 4—Interrupted tone detected: 60 or 120 interruptions per minute (IPM).

**Example** `voice-detection = 1`

**Location** CLT-RESULT

## vp-capability

**Description** Specifies whether a virtual private channel (VPC) can be established from the advertising node to the reachable address prefix.

**Usage** Select one of the following values:

- true—VPCs can be established.
- false—VPCs cannot be established. This is the default.

**Example** `set vp-capability = true`

**Location** PNNI-ROUTE-ADDR



## vpi

**Description** Specifies or indicates, according to the profile, the virtual path identifier (VPI) for an Asynchronous Transfer Mode (ATM) link, as follows:

- In the atm-options subprofile, vpi specifies the first side of the circuit.
- In the atm-connect-options subprofile, vpi specifies the second side of the circuit.
- In the outgoing-shaper subprofile, vpi specifies the VPI of the path whose traffic is shaped.
- In the atmpvc-stat and atmvc-stat profiles, the vpi value is read-only.

**Usage** Valid values are as follows:

- In an atm-options subprofile specify a number from 1 to 32767.
- In the atm-connect-options subprofile, specify a number from 0 to 255. The default is 0 (zero), which causes the unit to use virtual channel (VC) switching.
- In the atmpvc-stat and atmvc-stat profiles, the vpi value is read-only.

**Example** set vpi = 29

**Location** CONNECTION:atm-options  
 CONNECTION:atm-connect-options  
 ATMPVC-STAT  
 ATMVCC-STAT  
 SWITCH-CONFIG:atm-parameters:outgoing-shaper

**See Also** vci

## vpi-vci-range

**Description** Specifies a virtual path identifier-virtual channel identifier (VPI-VCI) range.

**Usage** You can use the vpi-vci-range value to select the best combination of VPI and VCI bit sizes to fit the list of supported VPI-VCI pairs obtained from the network provider. The new values take effect as soon as you write the profile. Following are the possible values:

| Value                  | VPI range | VCI range |
|------------------------|-----------|-----------|
| VPI-0-255-VCI-32-255   | 0-255     | 32-255    |
| VPI-0-255-VCI-32-511   | 0-255     | 32-511    |
| VPI-0-255-VCI-32-1023  | 0-255     | 32-1023   |
| VPI-0-255-VCI-32-2047  | 0-255     | 32-2047   |
| VPI-0-255-VCI-32-4095  | 0-255     | 32-4095   |
| VPI-0-255-VCI-32-8191  | 0-255     | 32-8191   |
| VPI-0-255-VCI-32-16383 | 0-255     | 32-16383  |

**Dependencies** Consider the following

- Before setting the `vpi-vci-range` value, make sure that there is only one VC-switching VPI for the port, and that the rest of the trunk ports in the system use less than 16K for the virtual channel connection (VCC). The system can handle a maximum 32K VCC for all trunk ports combined.
- The VCI range is valid only for VPIs assigned for VC switching by the `vc-switching-vci` setting. VPI 0 is always used for the VCC. There are no restrictions on the VCI range for VPIs that use VP switching.
- Exercise caution when changing the value of `vpi-vci-range`. Any increase in the range requires the unit to reserve more VCCs for the port, and all VPIs assigned for VC switching reserve the range. Therefore, the VCC numbers for the port increase with the number of VPIs assigned for the VCC.
- To change the value of `vpi-vci-range`, you must set `active` to `no` to put all of the affected connections out of service administratively.

**Location** AL-DMT-STAT

ATM-INTERNAL-STAT  
DS1-ATM-STAT  
DS3-ATM:line-config  
DS3-ATM-STAT  
E3-ATM:line-config  
E3-ATM-STAT  
HDSL2-STAT  
IMA-GROUP-STAT  
OC3-ATM:line-config  
OC3-ATM-STAT  
SDSL-STAT  
SHDSL-STAT  
SLOT-STATIC-CONFIG

**See Also** vci  
vpi

## vp-switching

**Description** Enables or disables virtual path (VP) switching for the first side of the circuit.

**Usage** Valid values are as follows:

- `yes`—Enables virtual path switching for the first side of the circuit. If this parameter is set to `yes`, you must enable virtual path switching on both sides of the circuit and specify a valid virtual path identifier (VPI) number for each side.
- `no` (the default)—Disables virtual path switching for the first side of the circuit.

**Example** `set vp-switching = no`

**Location** CONNECTION

**See Also** vp-switching-vpi  
vpi

## vp-switching-vpi

**Description** Specifies the virtual path identifier (VPI) to be used for virtual path (VP) switching on the interface.

**Usage** Specify a VPI from 1 to 31. The default is 15.

**Example** `set vp-switching-vpi = 15`

**Dependencies** In the `atm-internal` profile, this setting applies only to ISDN digital subscriber line (IDSL) line interface modules (LIMs). It does not apply to the router modules.

On an ATM interface of an external module, the rest of the VPI values in the `vpi-vci-range` specification for the interface are used for virtual channel switching.

**Location** `AL-DMT:line-config`

`AL-DMT-STAT`

`ATM-INTERNAL:line-config`

`ATM-INTERNAL-STAT`

`DS1-ATM:line-config`

`DS1-ATM-STAT`

`HDSL2:line-config`

`HDSL2-STAT`

`IMAGROUP`

`IMA-GROUP-STAT`

`SDSL:line-config`

`SDSL-STAT`

`SHDSL:line-config`

`SHDSL-STAT`

## vrouter

**Description** Specifies the name of a defined virtual router (VRouter). The effect varies by profile as follows:

- Specifying the VRouter name in a `connection` profile groups the WAN interfaces with the VRouter.
- Specifying the VRouter name in an `ip-interface` profile groups the LAN interfaces with the VRouter.
- Specifying the VRouter name in the `tunnel-options` subprofile defines the name of the VRouter to use for establishing a Layer 2 Tunneling Protocol (L2TP) tunnel.
- Specifying the name in an `ip-route` profile defines the name of the VRouter that owns the static route. The route will be part of the VRouter's routing table.

**Usage** Specify the name of a VRouter. The default is `null`, which specifies that the global VRouter is in use.

**Example** `set vrouter = vrouter2`

**Dependencies** Consider the following:

- L2TP tunnels can be built on specific VRouters. L2TP packets (control channel and encapsulated data) are sent by the configured VRouter for that tunnel. Because each VRouter maintains its own routing table and can detect only those interfaces that explicitly specify the same VRouter, this feature enables the system to separate traffic for different L2TP network server (LNS) systems.  
Note that a Stinger router module must dedicate one IP interface to each VRouter. In addition, the specified VRouter must reside on the L2TP access concentrator (LAC).
- You can use multiple VRouters with ATMP configurations by defining a VRouter in each connection profile.

**Location** CONNECTION  
CONNECTION:tunnel-options  
IP-INTERFACE  
IP-ROUTE

## vrouter-enabled

**Description** Read-only. Indicates the license status for the virtual router (VRouter) feature.

**Usage** Following are the valid values for this parameter:

- `yes`—The virtual router feature is enabled.
- `no`—The virtual router feature is disabled.

**Dependencies** This feature is available only on Stinger units equipped with a router module.

**Location** BASE

## vrouter-ip-addr

**Description** Specifies the system IP address for the virtual router.

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

**Example** `set vrouter-ip-addr = 200.40.60.5`

**Location** VROUTER

## W

### wan-line-state-change-enabled

**Description** Enables or disables trap (notification) generation if the state of an E1 or T1 line changes (Ascend trap 40). This trap sends the following information to the Simple Network Management Protocol (SNMP) manager:

- The T1 or E1 line interface index (wanLineIfIndex).
- The line usage (wanLineUsage). This usage is reported as trunk, quiesced, or disabled.
- The absolute time to show when the line state changed (sysAbsoluteCurrentTime).

**Usage** Valid values are as follows:

- `yes`—Enables trap generation if the state of an E1 or T1 line changes.
- `no` (the default)—Disables trap generation if the state of an E1 or T1 line changes.

**Example** `set wan-line-state-change-enabled = yes`

**Location** TRAP

### warmstart-enabled

**Description** Specifies whether the Stinger unit generates a trap (notification) when the unit reinitializes itself in such a way that neither the configuration of the SNMP manager nor of the unit itself is altered.

**Usage** Valid values are as follows:

- `yes` (the default)—Specifies that the system generates a trap when the Stinger unit reinitializes itself so that neither the configuration of the SNMP manager nor of the system itself is altered.
- `no`—Specifies that the system does not generate a trap when the Stinger unit reinitializes itself so that neither the configuration of the SNMP manager nor of the system itself is altered.

**Example** `set warmstart-enabled = no`

**Location** TRAP

**See Also** `coldstart-enabled`

### watchdog-name

**Description** Specifies an individual watchdog name.

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.

**Usage** Specify up to 80 characters. The default is a system-defined standard name.

**Example** `set watchdog-name = tempModule1`

**Location** WATCHDOG-CONFIG

## watchdog-trap-enable

**Description** Enables or disables the watchdog warning trap (notification) for the specified watchdog.

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.

**Usage** Valid values are as follows:

- `yes` (the default)—Enables the watchdog warning trap.
- `no`—Disables the watchdog warning trap.

**Example** `set watchdog-trap-enable = no`

**Location** WATCHDOG-CONFIG

## watchdog-type

**Description** Specifies the type of a watchdog.

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.

**Usage** Valid values are as follows:

- `other`—Other type of watchdog.
- `thermal`
- `fan`
- `fantray`
- `relay`
- `cbus`

**Example** `set watchdog-type = relay`

**Location** WATCHDOG-CONFIG:watchdog-index

## watchdog-warning-enabled

**Description** Specifies whether the SNMP watchdog-warning trap (notification) is enabled.

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.

**Usage** Valid values are as follows:

- `yes` (the default)—Specifies that the SNMP watchdog-warning trap is enabled.
- `no`—Specifies that the SNMP watchdog-warning trap is disabled.

**Example** set watchdog-warning-enabled = no

**Location** TRAP

## window-size

**Description** Specifies the size of the Q.SAAL window.

The signaling ATM adaptation layer (SAAL) provides reliable transport of q.2931 messages. Window size is typically related to an interval at which packets can be received or retransmitted. Standard algorithms are used to adjust window size according to network conditions.

**Usage** Valid values range from 16 to 128. The default value is 64.

**Example** set window-size = 50

**Location** ATM-IF-SIG-PARAMS [n] :qsaal-options

## working-channel

**Description** Read-only. Indicates the physical address of the working channel in an automatic protection switching (APS) system.

**Usage** If a switch has occurred, this read-only parameter is set to the address of the channel being switched. Otherwise, it is set to the value { any-shelf any-slot 0 }.

**Example** working-channel = { shelf-1 trunk-module-1 1 }

**Location** APS-STAT

## working-channel-signal-degrade-exponent

**Description** Specifies the signal degrade exponent for the working channel in automatic protection switching (APS).

**Usage** Specify a number from 5 through 9. The default is 6.

**Example** set working-channel-signal-degrade-exponent = 7

**Location** APS-CONFIG

## working-channel-signal-failure-exponent

**Description** Specifies the signal failure exponent for the working channel in automatic protection switching (APS).

**Usage** Specify a number from 3 through 5. The default is 3.

**Example** set working-channel-signal-failure-exponent = 4

**Location** APS-CONFIG

## write-access

**Description** Enables or disables write access to the SNMP agent in a Stinger unit for an SNMP manager on a remote host.

**Usage** Valid values are as follows:

- **yes**—Specifies that the SNMP agent allows write access in addition to read access.
- **no** (the default)—Specifies that the SNMP agent allows the SNMP manager only read access.

**Example** `set write-access = yes`

**Dependencies** For write-access to apply, active must be set to yes.

**Location** `SNMP-MANAGER`

## write-access-hosts

**Description** An array that consists of up to five IP addresses of SNMP managers that have SNMP write permission. The Stinger unit responds to SNMP Set, Get, and Get-Next commands from only the SNMP managers you specify.

**Usage** Each element in the array can specify an IP address. With SNMP as the working profile, use the List command to display the array elements. For example:

```
admin> list write-access-hosts
[in SNMP:write-access-hosts]
write-access-hosts[1] = 0.0.0.0
write-access-hosts[2] = 0.0.0.0
write-access-hosts[3] = 0.0.0.0
write-access-hosts[4] = 0.0.0.0
write-access-hosts[5] = 0.0.0.0
```

You can then set a write-access-hosts value by specifying its numeric index and entering an address. For example:

```
admin> set 1 = 10.2.3.4/24
```

Or, you can set an array element without first listing the array. For example:

```
admin> set write-access-hosts 1 = 10.2.3.4/24
```

```
admin> set write-access-hosts 2 = 10.5.6.7/29
```

**Dependencies** For the write-access-hosts parameter to restrict read-write access to the Stinger unit, you must set enforce-address-security to yes.

**Location** `SNMP-MANAGER`

## write-view-name

**Description** Specifies the name of a view for write access in a view-based access control model (VACM).

**Usage** Specify a name of up to 32 characters. If a request that matches the access-properties specified in this profile uses this name, read access is granted.



**Example** `set write-view-name = writeview1`

**Location** VACM-ACCESS

**See Also** `access-properties`

## wtr-timer-duration

**Description** Specifies the protection group waiting time to revert (WTR) in tens of milliseconds.

**Usage** Specify a number from 0 through 4,294,967,295. The default is 3000.

**Example** `set wtr-timer-duration = 3500`

**Dependencies** The `wtr-timer-duration` parameter cannot be set when `revertive-mode` is set to `non-revertive`.

**Location** APS-CONFIG

# X

## xmit-delay

**Description** Specifies the estimated number of seconds required to transmit a Link State Update (LSU) packet over an Open Shortest Path First (OSPF) virtual link interface. Before transmission, link state advertisements (LSAs) contained in the LSU packet have their ages incremented by the amount you specify.

**Usage** Specify a number greater than 0 (zero). The value you specify must take into account transmission and propagation delays. The default is 1.

**Example** `set xmit-delay = 8`

**Location** OSPF-VIRTUAL-LINK

## Y

### yellow-receive

**Description** Read-only. Indicates whether the local device has received a loss-of-frame (Yellow Alarm) indication. A Yellow Alarm indicates that a device on the line has detected framing errors in the signal.

**Usage** Valid values for this read-only setting are:

- `true`—Indicates that the local device has received a Yellow Alarm indication.
- `false`—Indicates that the local device has not received a Yellow Alarm indication.

**Example** `yellow-receive = false`

**Location** DS1-ATM-STAT

DS3-ATM-STAT

E3-ATM-STAT

OC3-ATM-STAT

**See Also** `ais-receive`

# Progress and Disconnect Codes

# 4

|                        |     |
|------------------------|-----|
| Progress codes .....   | 4-1 |
| Disconnect codes ..... | 4-3 |

## Progress codes

Table 4-1 explains the progress codes.

*Table 4-1. Progress codes*

| Code | Explanation                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0    | No progress.                                                                                                                                                                                                                                                                                                                                                                                                      |
| 1    | Not applicable.<br>A progress code 2 is a default values, literally indicating "unknown".<br>The unit displays "2" for progress codes that have not yet been explicitly defined.                                                                                                                                                                                                                                  |
| 2    | The progress of the call is unknown.<br>-----<br>*Shortly after answering the call, the TAOS unit could not detect any signal from the computer's modem. Typically, the modems had marginal line quality. Because the TAOS unit's modem has a digital connection to its local CO, the poor line quality is between the user's modem and its local CO. Also, there might be an incompatibility between the modems. |
| 40   | The terminal-server session has started up.                                                                                                                                                                                                                                                                                                                                                                       |
| 41   | The Stinger unit is establishing the TCP connection.                                                                                                                                                                                                                                                                                                                                                              |
| 42   | The Stinger unit is establishing the immediate Telnet connection.                                                                                                                                                                                                                                                                                                                                                 |
| 43   | The Stinger unit has established a raw TCP session with the host.<br>This code does not imply that the user has logged into the host.                                                                                                                                                                                                                                                                             |

Table 4-1. Progress codes (Continued)

| Code | Explanation                                                                                                                                     |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 44   | The Stinger unit has established an immediate Telnet connection with the host. This code does not imply that the user has logged into the host. |
| 45   | The Stinger unit is establishing an Rlogin session.                                                                                             |
| 46   | The Stinger unit has established an Rlogin session with the host. This code does not imply that the user has logged into the host.              |
| 47   | Terminal-server authentication has begun.                                                                                                       |
| 60   | The LAN session is up.                                                                                                                          |
| 61   | LCP negotiations are allowed.                                                                                                                   |
| 62   | CCP negotiations are allowed.                                                                                                                   |
| 63   | IPNCP negotiations are allowed.                                                                                                                 |
| 65   | LCP is in the open state.                                                                                                                       |
| 66   | CCP is in the open state.                                                                                                                       |
| 67   | IPNCP is in the open state.                                                                                                                     |
| 68   | BNCP is in the open state.                                                                                                                      |
| 69   | LCP is in the initial state.                                                                                                                    |
| 70   | LCP is in the starting state.                                                                                                                   |
| 71   | LCP is in the closed state.                                                                                                                     |
| 72   | LCP is in the stopped state.                                                                                                                    |
| 73   | LCP is in the closing state.                                                                                                                    |
| 74   | LCP is in the stopping state.                                                                                                                   |
| 75   | LCP is in the request sent state.                                                                                                               |
| 76   | LCP is in the ACK received state.                                                                                                               |
| 77   | LCP is in the ACK sent state.                                                                                                                   |
| 82   | BACP is being opened.                                                                                                                           |
| 83   | BACP is in an open state.                                                                                                                       |
| 84   | CBCP is being opened.                                                                                                                           |
| 85   | CBCP is in an open state.                                                                                                                       |

Table 4-1. Progress codes (Continued)

| Code | Explanation                                                        |
|------|--------------------------------------------------------------------|
| 90   | The unit has accepted a V.110 call.                                |
| 91   | The V.110 call is in an open state.                                |
| 92   | The V.110 call is in a carrier state.                              |
| 93   | The V.110 call is in a reset state.                                |
| 94   | The V.110 call is in a closed state.                               |
| 101  | Authentication failed.                                             |
| 102  | The remote authentication server timed out.                        |
| 420  | Control block is created.                                          |
| 421  | Control block is initialized in NBASE.                             |
| 422  | Call is pending UP state; TAOS call control is in progress.        |
| 423  | Call is Up.                                                        |
| 424  | Call is going down. TAOS call control in progress.                 |
| 425  | Call control needs to be deactivated.                              |
| 426  | Call is in connection admission control (CAC) stage.               |
| 427  | Call is in Restart stage.                                          |
| 428  | Call is in soft permanent virtual circuit (SPVC) management stage. |

## Disconnect codes

Table 4-2 explains the disconnect-cause codes.

Table 4-2. Disconnect codes

| Code | Description                                                                                                                                                                                                                          |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | This value is not applied to any call.                                                                                                                                                                                               |
| 2    | The disconnect occurred for an unknown reason. A cause code 2 or Progress code 2 are default values, literally indicating "unknown". The unit displays "2" for disconnects and progresses that have not yet been explicitly defined. |
| 3    | The call was disconnected.                                                                                                                                                                                                           |
| 4    | CLID authentication failed.                                                                                                                                                                                                          |

Table 4-2. Disconnect codes (Continued)

| Code | Description                                                                                                                                                                          |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5    | A RADIUS timeout occurred during authentication.                                                                                                                                     |
| 6    | The Stinger unit is establishing the TCP connection.                                                                                                                                 |
| 7    | The Pre-T310 Send Disc timer was triggered.                                                                                                                                          |
| 20   | The user exited normally from the terminal server.                                                                                                                                   |
| 21   | The terminal server timed out waiting for user input.                                                                                                                                |
| 22   | A forced disconnect occurred when the user exited a Telnet session.                                                                                                                  |
| 23   | No IP address was available when the user entered the SLIP command.                                                                                                                  |
| 24   | A forced disconnect occurred when the user exited a raw TCP session.                                                                                                                 |
| 25   | The user exceeded the limit for login attempts.                                                                                                                                      |
| 26   | The unit attempted to start a raw TCP session, but raw TCP is disabled.                                                                                                              |
| 27   | Control-C characters were received during the login.                                                                                                                                 |
| 28   | The terminal-server session cleared ungracefully.                                                                                                                                    |
| 29   | The user closed a terminal-server virtual connection normally.                                                                                                                       |
| 30   | The terminal-server virtual connection cleared ungracefully.                                                                                                                         |
| 31   | The user exited from an Rlogin session.                                                                                                                                              |
| 32   | The establishment of the Rlogin session failed because of bad options.                                                                                                               |
| 33   | The unit lacks the resources to process a terminal-server request.                                                                                                                   |
| 35   | The MP+ session cleared because no null MP packets were received. A unit sends (and should receive) null MP packets throughout an MP+ session.                                       |
| 40   | LCP timed out waiting for a response.                                                                                                                                                |
| 41   | LCP negotiations failed, probably because the user is configured to send passwords by means of PAP, and the unit is configured to accept passwords by means of CHAP (or vice versa). |
| 42   | PAP authentication failed.                                                                                                                                                           |

Table 4-2. Disconnect codes (Continued)

| Code | Description                                                                                                                                                                                             |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 43   | CHAP authentication failed.                                                                                                                                                                             |
| 44   | Authentication failed from a remote server.                                                                                                                                                             |
| 45   | The unit received a Terminate Request packet while LCP was in an open state.                                                                                                                            |
| 46   | The unit received a Close Request from an upper layer, indicating graceful LCP closure.                                                                                                                 |
| 47   | The unit cleared the call because no Network Core Protocols (NCPs) were successfully negotiated. Typically, there is no agreement on the type of routing or bridging that is supported for the session. |
| 48   | An MP session was disconnected. The unit accepted an added channel, but cannot determine to which call to add the new channel.                                                                          |
| 49   | The unit disconnected an MP call because no more channels could be added.                                                                                                                               |
| 50   | Telnet or raw TCP session tables are full.                                                                                                                                                              |
| 51   | The unit has exhausted Telnet or raw TCP resources.                                                                                                                                                     |
| 52   | For a Telnet or raw TCP session, the IP address is invalid.                                                                                                                                             |
| 53   | The unit cannot resolve the host name for a Telnet or raw TCP session.                                                                                                                                  |
| 54   | For a Telnet or raw TCP session, the unit received a bad or missing port number.                                                                                                                        |
| 60   | For a Telnet or raw TCP session, the host was reset.                                                                                                                                                    |
| 61   | For a Telnet or raw TCP session, the connection was refused.                                                                                                                                            |
| 62   | For a Telnet or raw TCP session, the connection timed out.                                                                                                                                              |
| 63   | For a Telnet or raw TCP session, the connection was closed by a foreign host.                                                                                                                           |
| 64   | For a Telnet or raw TCP session, the network was unreachable.                                                                                                                                           |
| 65   | For a Telnet or raw TCP session, the host was unreachable.                                                                                                                                              |
| 66   | For a Telnet or raw TCP session, the network admin was unreachable.                                                                                                                                     |

Table 4-2. Disconnect codes (Continued)

| Code | Description                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------|
| 67   | For a Telnet or raw TCP session, the host admin was unreachable.                                                                      |
| 68   | For a Telnet or raw TCP session, the port was unreachable.                                                                            |
| 100  | The session timed out.                                                                                                                |
| 101  | The user name was invalid.                                                                                                            |
| 115  | The dial-in user is no longer active.                                                                                                 |
| 120  | A requested protocol is disabled or unsupported.                                                                                      |
| 150  | A disconnect was requested by the RADIUS server.                                                                                      |
| 151  | The call was disconnected by the local administrator.                                                                                 |
| 152  | The call was disconnected by means of SNMP.                                                                                           |
| 160  | The unit exceeded the maximum number of V.110 retries.                                                                                |
| 170  | A timeout occurred while the unit waited for the remote device to be authenticated.                                                   |
| 181  | The call was cleared by the system.                                                                                                   |
| 185  | The signal was lost from remote end, probably because the remote end's modem was turned off.                                          |
| 190  | The resource has been quiesced.                                                                                                       |
| 195  | The maximum duration for the call has been reached.                                                                                   |
| 201  | The unit has low memory.                                                                                                              |
| 230  | The unit deleted the Virtual Router (VRouter).                                                                                        |
| 240  | The unit disconnected the call on the basis of LQM measurements.                                                                      |
| 241  | The unit cleared a backup call.                                                                                                       |
| 1031 | CAC failure due to internal system resources.                                                                                         |
| 1032 | Bandwidth failure on the egress.                                                                                                      |
| 1033 | Bandwidth failure on the ingress.                                                                                                     |
| 1034 | Slot bandwidth failure. Bandwidth is defined by the allow-guaranteed-up-stream-bandwidth parameter of the slot-static-config profile. |



Table 4-2. Disconnect codes (Continued)

| Code | Description                                                                                                   |
|------|---------------------------------------------------------------------------------------------------------------|
| 1035 | LIM port bandwidth failure.                                                                                   |
| 1036 | OLIM port bandwidth failure.                                                                                  |
| 1037 | Cascaded Stinger MRT port bandwidth failure.                                                                  |
| 1038 | OLIM slot bandwidth failure.                                                                                  |
| 1039 | A VPI used for a VCC is not within the valid range defined in by the <code>vc-switching-vpi</code> parameter. |
| 1040 | VPI/VCI is not valid for VC switching.                                                                        |
| 1041 | VPI is assigned to a VCC; it cannot be used in a VPC.                                                         |
| 1042 | The ingress LIM has low memory.                                                                               |

